



Dr. Vishwanath Karad

**MIT WORLD PEACE  
UNIVERSITY** | PUNE

TECHNOLOGY, RESEARCH, SOCIAL INNOVATION & PARTNERSHIPS

## **Project Report**

on

## **Fully Homomorphic Encryption In Nuclear Power Plants**

Submitted by

**Project Members**

Hritika Kalghatgi	1032191063
Anshul Jaiswal	1032191332
Kushagra Amlani	1032192138
Khush Advani	1032191624

**Under the Internal Guidance of**

**Dr. Sukhada Bhingarkar**

**Under the External Guidance of**

**Dr. Hrishikesh Dewan**

**School of Computer Engineering and Technology**

**MIT World Peace University, Kothrud,**

**Pune 411 038, Maharashtra - India**

**2022-2023**



Dr. Vishwanath Karad

**MIT WORLD PEACE  
UNIVERSITY** | PUNE

TECHNOLOGY, RESEARCH, SOCIAL INNOVATION & PARTNERSHIPS

## SCHOOL OF COMPUTER ENGINEERING AND TECHNOLOGY

### C E R T I F I C A T E

This is to certify that,

**Hritika Kalghatgi**

of BTech. (Computer Science & Engineering) have completed their project titled  
*“Fully Homomorphic Encryption In Nuclear Power Plants”* and have submitted this Capstone  
Project Report towards fulfillment of the requirement for the Degree-Bachelor of Computer  
Science & Engineering (BTech-CSE) for the academic year 2022-2023.

**[Dr Sukhada Bhingarkar]**

Project Guide

School of CET

MIT World Peace University, Pune

**[Dr. Vrushali Kulkarni]**

Program Head

School of CET

MIT World Peace University, Pune

Internal Examiner:

External Examiner:

**Date:**



Dr. Vishwanath Karad

**MIT WORLD PEACE  
UNIVERSITY** | PUNE

TECHNOLOGY, RESEARCH, SOCIAL INNOVATION & PARTNERSHIPS

## SCHOOL OF COMPUTER ENGINEERING AND TECHNOLOGY

### C E R T I F I C A T E

This is to certify that,

**Anshul Jaiswal**

of BTech. (Computer Science & Engineering) have completed their project titled  
*“Fully Homomorphic Encryption In Nuclear Power Plants”* and have submitted this Capstone  
Project Report towards fulfillment of the requirement for the Degree-Bachelor of Computer  
Science & Engineering (BTech-CSE) for the academic year 2022-2023.

**[Dr Sukhada Bhingarkar]**

Project Guide

School of CET

MIT World Peace University, Pune

**[Dr. Vrushali Kulkarni]**

Program Head

School of CET

MIT World Peace University, Pune

Internal Examiner:

External Examiner:

**Date:**



Dr. Vishwanath Karad  
**MIT WORLD PEACE**  
**UNIVERSITY** | PUNE  
TECHNOLOGY, RESEARCH, SOCIAL INNOVATION & PARTNERSHIPS

## SCHOOL OF COMPUTER ENGINEERING AND TECHNOLOGY

### C E R T I F I C A T E

This is to certify that,

**Khush Advani**

of BTech. (Computer Science & Engineering) have completed their project titled  
“Fully Homomorphic Encryption In Nuclear Power Plants” and have submitted this Capstone  
Project Report towards fulfillment of the requirement for the Degree-Bachelor of Computer  
Science & Engineering (BTech-CSE) for the academic year 2022-2023.

**[Dr Sukhada Bhingarkar]**

Project Guide

School of CET

MIT World Peace University, Pune

**[Dr. Vrushali Kulkarni]**

Program Head

School of CET

MIT World Peace University, Pune

Internal Examiner:

External Examiner:

**Date**



Dr. Vishwanath Karad

**MIT WORLD PEACE  
UNIVERSITY** | PUNE

TECHNOLOGY, RESEARCH, SOCIAL INNOVATION & PARTNERSHIPS

## SCHOOL OF COMPUTER ENGINEERING AND TECHNOLOGY

### C E R T I F I C A T E

This is to certify that,

**Kushagra Amlani**

of BTech. (Computer Science & Engineering) have completed their project titled  
*“Fully Homomorphic Encryption In Nuclear Power Plants”* and have submitted this Capstone  
Project Report towards fulfillment of the requirement for the Degree-Bachelor of Computer  
Science & Engineering (BTech-CSE) for the academic year 2022-2023.

**[Dr Sukhada Bhingarkar]**

Project Guide

School of CET

MIT World Peace University, Pune

**[Dr. Vrushali Kulkarni]**

Program Head

School of CET

MIT World Peace University, Pune

Internal Examiner:

External Examiner:

**Date:**

# Acknowledgement

We would like to express our heartfelt gratitude to our college for providing us with the opportunity to undertake this group project on homomorphic encryption. The project has been an invaluable experience, allowing us to delve into the fascinating world of cryptography and explore the potential applications of homomorphic encryption.

We extend our sincere appreciation to our project coordinator, Dr Sukhada Bhingarkar, for their constant guidance and support throughout this project. Their expertise, enthusiasm, and dedication to teaching have been instrumental in shaping our understanding of homomorphic encryption and its significance in modern data security. Their insightful suggestions, constructive feedback, and willingness to answer our queries have immensely contributed to the success of this project.

Furthermore, we would like to thank Ziroh Labs for their valuable support and collaboration in our project. Their involvement has provided us with invaluable industry insights and practical perspectives on the implementation of homomorphic encryption. The resources, guidance, and expertise shared by Ziroh Labs have greatly enriched our project experience and expanded our knowledge in this field.

We also want to acknowledge the resources and references provided by the college library and online platforms that aided us in acquiring the necessary knowledge and understanding of homomorphic encryption.

This project has been an enriching experience that has not only expanded our knowledge but also honed our teamwork and problem-solving skills. We sincerely thank everyone involved in making this project a success, including our college, our teacher, and Ziroh Labs, for their valuable contributions and guidance throughout our journey.

## **Name of the Students:**

Hritika Kalghatgi

Anshul Jaiswal

Khush Advani

Kushagra Amlani

# Abstract

The unique challenges and requirements of the nuclear power industry demand robust security measures to protect sensitive data and ensure the integrity of critical systems. Maintaining security and confidentiality in a nuclear power plant is of paramount importance due to the potential consequences of cyber security attacks. Nuclear power plants contain critical infrastructure and highly sensitive systems that, if compromised, can pose significant risks to public safety and health. Integration calculations are essential in various computations for safety analysis, risk assessment, and regulatory compliance in nuclear power plants. However, the sensitive nature of the data involved raises concerns regarding data privacy and security. This paper proposes the adoption of Fully Homomorphic Encryption (FHE) as a powerful cryptographic solution for secure computation on encrypted data. FHE enables the execution of various operations on encrypted data, preserving data privacy throughout the computation process. To evaluate the performance and feasibility of the proposed scheme, we have shown a novel methodology using Ziroh Labs' FHE Libraries with experimental results. The values calculated using FHE secure computation and normal integration on unsecured data show minimal variation, proving that integration is also an operation that can be carried forward on encrypted data, uplifting data privacy.

**Keywords** —Data Confidentiality, Data Integrity, Data Privacy, Fully Homomorphic Encryption, Nuclear Power Plants

# List of Figures

## **Part A**

<b>5.1</b>	Use Case Diagram	34
<b>5.2</b>	Activity Diagram	35
<b>5.3</b>	Class Diagram	36
<b>7.1</b>	Graph of simple single variable curve using Monte Carlo integration	42
<b>7.2</b>	Graph of polynomial curve using Monte Carlo integration	43
<b>7.3</b>	Graph of sin curve with Monte Carlo integration	45
<b>8.1</b>	Graph representing the time needed for every integration equation to be solved with FHE and without FHE.	46
<b>8.2</b>	GUI Main screen for user to begin	51
<b>8.3</b>	.GUI Choice screen for user to select which type of integration they want to perform.	51
<b>8.4</b>	GUI Input screen asking user to enter no. of random points t generate.	52
<b>8.5</b>	GUI Output screen with integration result using FHE	52

## **Part B : Individual Project Report**

<b>4.1</b>	Class Diagram of Module	
<b>4.2</b>	Graph of simple single variable curve using Monte Carlo integration	74
<b>4.3</b>	Graph of polynomial curve using Monte Carlo integration	75
<b>4.4</b>	Graph of sin curve with Monte Carlo integration	76
<b>4.5</b>	Graph representing the time needed for every integration equation to be solved with FHE and without FHE.	78



# List of Tables

## **Part A**

<b>8.2</b>	Table of Accuracy	46
<b>8.2</b>	Tables for time difference between FHE and no FHE	48

## **Part B : Individual Project Report**

<b>4.1</b>	Table of Accuracy	78
<b>4.2</b>	Tables for time difference between FHE and no FHE	80

# Contents

Acknowledgement .....	I
Abstract .....	II
List of Figures .....	III
List of Tables .....	IV

## **PART A**

<b>01</b>	<b>Introduction</b>	<b>1</b>
	1.1 Homomorphic Encryption	1
	1.1.1 Partial Homomorphic Encryption	1
	1.1.2 Somewhat Homomorphic Encryption	3
	1.1.3 Fully Homomorphic Encryption	5
	1.2 Problem Statement	8
	1.3 Objectives	8
	1.4 Scope	10
<b>02</b>	Literature Survey	12
<b>03</b>	Problem Statement	25
	3.1 Project Objectives	25
	3.2 Project Assumptions	26
	3.3 Challenges and Considerations	27
	3.4 Project Limitations	29
<b>04</b>	Project Requirements	31
	4.1 Human Resources	31

	4.2	Reusable Software Components		31
	4.3	Software And Hardware Requirement		32
	4.4	Other Requirements		32
<b>05</b>	System Design Proposed Architecture			33
	5.1	Hardware Requirements		33
	5.2	Software Requirements		33
	5.3	UML Diagrams		34
		5.3.1	Use case Diagram	34
		5.3.2	Activity Diagram	35
		5.3.3	Class Diagram	36
<b>06</b>	Project Plan			37
	6.1	Project Initiation Phase		37
	6.2	Requirements Gathering and Analysis		37
	6.3	Design and Development Phase		37
	6.4	Testing and Quality Assurance		38
	6.5	Documentation and Finalization		38
<b>07</b>	Methodology			39
	7.1	Proposed Work		39
	7.2	Scenarios and algorithms		41
		7.2.1	Scenario Of Simple Integration	41
		7.2.2	Scenario Of Polynomial Integration	42
		7.2.3	Scenario Of Sin Function Integration	43
<b>08</b>	Implementation and Result			45

## Fully Homomorphic Encryption in Nuclear Power Plants

	8.1	Integration accuracy	46
	8.2	GUI Implementation	49
	8.3	Advantages	53
<b>09</b>	Future Prospects		54
<b>10</b>	Limitations		57
<b>11</b>	Conclusion		59
<b>12</b>	References		61
<b>13</b>	Appendices		64
	13.1	Base Paper(s)	64
	13.2	Plagiarism Report	65

## **PART B : Individual Project Report**

<b>01</b>	Problem Statement		69
<b>02</b>	Module Objectives		70
<b>03</b>	Module Scope		71
<b>04</b>	Module		72
	4.1	Hardware & Software requirements	72
	4.2	Module Interfaces	72
	4.3	Module Dependencies	73
	4.4	Module Design	74
	4.5	Module Implementation	74
	4.6	Testing & Results	78
<b>05</b>	Conclusion		83

# Chapter 1

## INTRODUCTION

Data privacy is important in nuclear power plants for several reasons[8]. Firstly, nuclear power plants process and store a large amount of sensitive information, such as reactor design data, safety procedures, and operational parameters.

This information is critical to the safe and efficient operation of the plant, and unauthorized access to this information can have serious consequences, including safety risks and economic damage.

Secondly, nuclear power plants are often targeted by cyberattacks, which can compromise the integrity and confidentiality of their data. Malicious actors may attempt to steal sensitive information or disrupt plant operations, which can result in safety risks, equipment damage, or even a nuclear accident.[8]

Homomorphic encryption can be used to protect sensitive data, such as reactor operational parameters and safety procedures, from unauthorized access and cyberattacks[7].

We plan on successfully running calculations and operations which involve integration and calculus required for the proper functioning of a nuclear power plant on encrypted data which promotes the confidentiality and security of the entire facility.

### 1.1 Homomorphic Encryption

Homomorphic encryption is a cryptographic technique that allows performing computations on encrypted data without decrypting it first[13]. This property is particularly useful in scenarios where data privacy is a concern, as it enables computations on sensitive data without exposing each with its own strengths and limitations. Here are the three main types of homomorphic encryption:

#### 1.1.1 Partially Homomorphic Encryption:

Partially Homomorphic Encryption (PHE) is a type of homomorphic encryption scheme that allows computations on encrypted data, but only for a specific operation, either addition or multiplication[13]. The two common types of partially homomorphic encryption are:

### 1. Additive Homomorphic Encryption:

Additive homomorphic encryption schemes enable computations involving addition on encrypted data. The encryption process converts plaintext values into ciphertexts using a specific encryption algorithm. The ciphertexts can be added together directly without the need for decryption, and when the resulting ciphertext is decrypted, the plaintext sum of the original values is obtained.

To perform addition on encrypted data, the following steps are typically involved:

Encryption: Given two plaintext values, say  $a$  and  $b$ , each plaintext value is encrypted individually, resulting in two corresponding ciphertexts, let's call them  $\text{Enc}(a)$  and  $\text{Enc}(b)$ .

Addition: The ciphertexts  $\text{Enc}(a)$  and  $\text{Enc}(b)$  are combined using the encryption scheme's addition operation. This operation allows the ciphertexts to be added together, resulting in a new ciphertext, let's call it  $\text{Enc}(a + b)$ .

Decryption: The resulting ciphertext  $\text{Enc}(a + b)$  can be decrypted using the decryption algorithm of the encryption scheme, revealing the plaintext sum of  $a$  and  $b$ .

The additive homomorphic property is particularly useful when the computations primarily involve summation operations, such as aggregating data or computing simple statistics.

### 2. Multiplicative Homomorphic Encryption:

Multiplicative homomorphic encryption schemes allow computations involving multiplication on encrypted data. The encryption process transforms plaintext values into ciphertexts using a specific encryption algorithm. With multiplicative homomorphic encryption, ciphertexts can be multiplied together, and the decryption of the resulting ciphertext yields the product of the original plaintext values.

The steps involved in performing multiplication on encrypted data are as follows:

Encryption: Given two plaintext values, say  $a$  and  $b$ , each plaintext value is encrypted individually, resulting in two corresponding ciphertexts, let's call them  $\text{Enc}(a)$  and  $\text{Enc}(b)$ .

**Multiplication:** The ciphertexts  $\text{Enc}(a)$  and  $\text{Enc}(b)$  are combined using the encryption scheme's multiplication operation. This operation allows the ciphertexts to be multiplied together, resulting in a new ciphertext, let's call it  $\text{Enc}(a * b)$ .

**Decryption:** The resulting ciphertext  $\text{Enc}(a * b)$  can be decrypted using the decryption algorithm of the encryption scheme, revealing the plaintext product of  $a$  and  $b$ .

However, it's worth noting that performing multiple multiplications in succession with multiplicative homomorphic encryption can lead to a significant increase in the ciphertext size due to noise accumulation. This exponential growth in ciphertext size makes it less practical for certain applications.

In summary, partially homomorphic encryption allows computations on encrypted data for either addition or multiplication operations[13]. Additive homomorphic encryption supports addition computations directly on ciphertexts, while multiplicative homomorphic encryption allows multiplication computations. Both types of partially homomorphic encryption have their specific use cases and limitations, and they provide a foundation for more advanced homomorphic encryption schemes like fully homomorphic encryption.

### 1.1.2 Somewhat Homomorphic Encryption:

Somewhat Homomorphic Encryption (SWHE) is a type of homomorphic encryption scheme that allows limited computations on both addition and multiplication operations on encrypted data[13]. It strikes a balance between functionality and efficiency, providing a useful level of homomorphic computation while maintaining practicality.

Details of SWHE are:

**Encryption and Decryption:**

Like other homomorphic encryption schemes, SWHE involves an encryption algorithm and a corresponding decryption algorithm. The encryption algorithm takes a plaintext message as input and produces a ciphertext. The decryption algorithm, on the other hand, takes a ciphertext as input and recovers the original plaintext message.

**Homomorphic Operations:**

SWHE allows computations on encrypted data for both addition and multiplication, but there are limitations on the number of operations that can be performed or the types of operations that can be supported.

### a. Addition:

With SWHE, one can perform addition operations on encrypted data. The encryption scheme supports adding two ciphertexts together, resulting in a new ciphertext that, when decrypted, reveals the sum of the corresponding plaintexts. This property enables computations involving addition, such as calculating sums or aggregating data.

### b. Multiplication:

SWHE also supports limited multiplication operations on encrypted data. However, the number of multiplications that can be performed is typically constrained, and performing multiple multiplications in succession may introduce noise and affect the accuracy of the decrypted result.

### Noise Accumulation and Accuracy:

In SWHE, the encryption process introduces noise into the ciphertext. As computations are performed on encrypted data, this noise accumulates and affects the accuracy of the decrypted result. The noise accumulation is typically controlled to a certain level to ensure the correctness of the computations. Beyond a certain threshold, the noise may grow significantly, leading to unreliable decryption results.

### Use Cases:

Somewhat homomorphic encryption finds applications in scenarios where limited computations on encrypted data are required[13]. While it may not support arbitrary computations like fully homomorphic encryption, it is still useful in various practical scenarios. Some examples include:

- Secure computation on private data: SWHE enables performing calculations on encrypted sensitive data without revealing the underlying information, allowing privacy-preserving computations.
- Outsourcing computations: It allows delegating computations to untrusted parties while keeping the data confidential. The party can perform the computations on encrypted data and provide the encrypted results without accessing the plaintext.



- Secure data processing in cloud environments: SWHE can be employed to process encrypted data in cloud environments, allowing users to maintain control over their data while still benefiting from cloud computing capabilities.

It's important to note that the limitations of SWHE, such as restricted multiplication capabilities and noise accumulation, have led to the development of more advanced homomorphic encryption schemes, such as Fully Homomorphic Encryption (FHE), which overcome these limitations and provide more extensive computation capabilities on encrypted data. Nonetheless, SWHE serves as a practical and efficient solution for certain use cases that require limited homomorphic computations.

### 1.1.3 Fully Homomorphic Encryption:

Fully Homomorphic Encryption (FHE) is an advanced cryptographic technique that allows arbitrary computations to be performed on encrypted data without the need for decryption[13]. It is the most powerful type of homomorphic encryption, providing a comprehensive solution for secure computation on sensitive information. FHE in more detail:

Encryption and Decryption:

FHE involves an encryption algorithm and a corresponding decryption algorithm. The encryption algorithm takes a plaintext message as input and produces a ciphertext. The decryption algorithm, which is typically performed by the data owner or an authorized party, takes a ciphertext as input and recovers the original plaintext message.

Homomorphic Operations:

FHE supports arbitrary computations on encrypted data, including both addition and multiplication operations. This means that any computation that can be performed on plaintext data can also be executed on encrypted data, without the need to decrypt it.

a. Addition:

FHE allows computations involving addition on encrypted data. Ciphertexts representing encrypted values can be added together, resulting in a new ciphertext that, when decrypted, reveals the sum of the corresponding plaintext values.

### b. Multiplication:

FHE enables computations involving multiplication on encrypted data. Ciphertexts representing encrypted values can be multiplied together, resulting in a new ciphertext that, when decrypted, reveals the product of the corresponding plaintext values.

Additionally, FHE allows for the composition of multiple additions and multiplications, enabling complex computations on encrypted data.

### Noise Management and Bootstrapping:

In FHE, noise is introduced during the encryption process, and as computations are performed on encrypted data, this noise accumulates. The accumulation of noise can impact the accuracy of the decrypted result. To address this issue, FHE schemes employ noise management techniques, such as modulus switching and relinearization, to control and reduce the noise level without compromising the security of the encryption scheme.

Bootstrapping is a crucial process in FHE that allows for the renewal of ciphertexts during computation[14], effectively resetting the noise accumulation. It enables the execution of an unlimited number of operations on encrypted data by refreshing the ciphertexts while preserving the security guarantees of the encryption scheme. Bootstrapping is typically computationally expensive and adds to the complexity of FHE implementations.

### Practical Considerations:

FHE is a powerful cryptographic tool, but it comes with some practical considerations:

#### a. Computational Complexity:

FHE schemes can be computationally expensive compared to other encryption schemes. Performing computations on encrypted data requires additional computational resources and may introduce latency in applications.

#### b. Ciphertext Expansion:

The size of the ciphertext can increase significantly with each operation performed. This expansion in ciphertext size can impact the efficiency and practicality of FHE in

certain scenarios.

### c. Key Management:

FHE involves the generation and management of encryption keys, which are crucial for the security and functionality of the scheme. Proper key management practices are essential to maintain the integrity and privacy of the encrypted data.

### Use Cases:

FHE has numerous potential applications[1], including:

- Secure cloud computing: FHE allows users to perform computations on encrypted data stored in the cloud, ensuring privacy and confidentiality.
- Privacy-preserving data analysis: FHE enables performing analytics on sensitive data without exposing the underlying information, making it valuable for applications in healthcare, finance, and other industries.
- Secure machine learning: FHE can be applied to train models and perform predictions on encrypted data while preserving privacy and confidentiality.
- Secure outsourcing of computations: FHE allows delegating computations to untrusted third parties while maintaining the confidentiality of the data being processed.

Fully Homomorphic Encryption represents a significant advancement in cryptographic techniques, providing a powerful tool for secure computation on encrypted data. Ongoing research aims to improve the efficiency and practicality of FHE, making it more accessible for real-world applications.

## 1.2 Problem Statement

For safe and effective operation, nuclear power plants depend on precise calculations. These computations use sophisticated mathematical techniques, such integration, to analyse a variety

of parameters and forecast results. Data privacy and security issues arise from the requirement to protect sensitive data, such as decay constants and other operational variables[10]. The solution is provided by FHE, which makes it possible to do computations on encrypted data without first having to decode it. The goal of this work is to use FHE to execute integration computations while protecting the privacy of sensitive information, making sure that all legal requirements are met, and maintaining operational security.

### 1.3 Objectives

Applying Homomorphic Encryption (HE) in nuclear power plants is driven by several key objectives. These objectives aim to address the challenges associated with data security, privacy, and computational integrity in nuclear power plant operations. The objectives of this project are as follows:

#### **Confidentiality of Sensitive Data:**

One of the primary objectives of applying HE in nuclear power plants is to ensure the confidentiality of sensitive data. Nuclear power plants handle critical information related to operations, control systems, safety protocols, and sensitive measurements. By encrypting the data using HE, the information remains confidential, even during computations and data processing. This objective prevents unauthorized access, data breaches, or information leaks that could compromise the security of the plant.

#### **Privacy-Preserving Data Analysis:**

HE enables privacy-preserving data analysis, allowing for secure computations on encrypted data. By applying HE to nuclear power plant data, operators can perform data analysis, anomaly detection, and optimization without exposing the underlying sensitive information. This objective safeguards the privacy of the data, ensuring that insights can be gained from the data without compromising the confidentiality of the plant's operations.

#### **Secure Outsourcing of Computations:**

HE provides a means to securely outsource computations to third-party service providers or cloud environments. By encrypting the data, nuclear power plants can delegate computations while maintaining the confidentiality and integrity of the sensitive information. This objective

enables efficient utilization of external computing resources without exposing the underlying data to potential security risks.

Fully homomorphic encryption is a potent tool for computation that protects privacy since it enables computations to be done directly on encrypted material without having to first decrypt it. With the help of the FHE method, operations like addition, multiplication, and comparison can be performed on encrypted data while still guaranteeing data confidentiality. The FHE libraries from Ziroh Lab were created with the goal of making it easier to construct FHE schemes by giving a foundation for safe and effective calculations on encrypted data.

### **Computational Integrity:**

Another objective of applying HE in nuclear power plants is to ensure the computational integrity of data processing. HE enables computations to be performed on encrypted data without the need for decryption. This objective ensures that the computations are carried out accurately and securely, eliminating the risk of tampering or unauthorized modifications to the data during processing.

### **Regulatory Compliance:**

Nuclear power plants operate within strict regulatory frameworks and compliance requirements to ensure the safety, security, and privacy of operations and data. Applying HE helps meet these regulatory obligations by providing a secure and privacy-preserving mechanism for data processing. This objective ensures that the use of HE aligns with industry standards, data protection regulations, and privacy laws, maintaining compliance with the applicable regulations.

### **Minimization of Data Exposure:**

By applying HE, nuclear power plants aim to minimize the exposure of sensitive data. Encrypted data can be processed and analyzed without the need to decrypt it, reducing the instances where the data is exposed in its unencrypted form. This objective reduces the attack surface and potential vulnerabilities, enhancing the overall security posture of the plant's operations.

### **Collaboration and Data Sharing:**

Applying HE also promotes collaboration and secure data sharing within the nuclear power

industry. Encrypted data can be securely shared with authorized parties or research institutions without revealing the underlying sensitive information. This objective facilitates knowledge sharing, research collaborations, and advancements in nuclear power plant operations while preserving the privacy and confidentiality of the data.

By achieving these objectives, applying Homomorphic Encryption (HE) in nuclear power plants enhances data security, privacy, computational integrity, and regulatory compliance. It enables secure and privacy-preserving data processing, analysis, and collaboration, contributing to the overall safety, efficiency, and integrity of nuclear power plant operations.

### 1.4 Scope

The scope of this project is as follows:

- **Secure data sharing:** Nuclear power plants generate a significant amount of sensitive data, including operational parameters, sensor readings, and safety reports. FHE can enable secure sharing of this data with external parties, such as regulatory bodies or third-party auditors, while preserving confidentiality. Encrypted data can be processed by the external entities without the need for decryption, ensuring data privacy.
- **Secure computation outsourcing:** Nuclear power plants often need to collaborate with external entities for specialized analysis or computational tasks. With FHE, they can securely outsource these computations to external service providers without exposing the underlying data. This allows for efficient data analysis while maintaining privacy and confidentiality.
- **Enhanced cybersecurity:** FHE can help protect critical infrastructure within nuclear power plants by securing sensitive algorithms[8], intellectual property, and software updates. By performing computations on encrypted data, FHE can prevent unauthorized access to algorithms or data leakage during transmission.
- **Data integrity verification:** FHE can be used to verify the integrity of critical data and ensure that it has not been tampered with during transmission or storage[5]. By performing computations on encrypted data, FHE can generate proofs that the results are correct without exposing the actual data.

- **Privacy-preserving analytics:** Nuclear power plants can use FHE to perform advanced analytics on sensitive data without compromising privacy[5]. For example, they can analyze historical operational data while keeping it encrypted, extracting valuable insights without exposing the underlying details.

# Chapter 2

## LITERATURE REVIEW

In this section, we will review and analyze existing research and studies that explore the various applications of FHE in different domains. The survey will encompass a wide range of topics, including FHE algorithms, implementation frameworks, security considerations, performance evaluations, and case studies. By examining the current state-of-the-art in FHE within the context of multiple domains, we aim to identify the strengths, limitations, and potential challenges associated with the adoption of this cryptographic technique in such critical infrastructures. We will also look into the related work that has been done in the field of cyber security in Nuclear Power Plants.

R. Sendhil et al. [3] highlight the benefits of homomorphic encryption in fog computing environments. By leveraging homomorphic encryption, fog nodes can perform computations on encrypted data received from fog devices, thereby preserving data privacy and security. This approach eliminates the need for data decryption at the fog nodes, minimizing the exposure of sensitive information to potential adversaries.

Zainab H. Mahmood et al. [4] present a novel approach for achieving noise-free homomorphic encryption using chaotic systems. The paper addresses the limitations of existing homomorphic encryption schemes that suffer from noise amplification during the evaluation process, leading to reduced accuracy and reliability. The proposed method utilizes chaotic systems to generate noise-free ciphertexts and achieves homomorphic operations with high precision. The proposed algorithm considers a noise-free algorithm, encrypted the plain text message as a matrix vector instead of one value at a time, and generates the ciphertext in floating-point numbers to unauthorized parties without data privacy leakages.

Amina Bel Korchi et al. [5] describe a novel use case of homomorphic encryption utilizing the Fan and Vercauteren (FV) cryptosystem, as well as a practical implementation of the FV cryptosystem and its use in an IoT use case. Shipowners may use their implementation to alter



encrypted data while respecting company competitiveness and without compromising security, privacy, or anonymization.

Jonathan West et al [6] provide a method for identifying essential digital assets within a nuclear reactor. This study presents three variants of this method. The runtime of these three solutions is acquired to show how each grows as the network model sizes for nuclear reactors get larger. Infall Syafalni et al. [7] describe a cloud security approach that uses homomorphic encryption for data analytics in the cloud. The experimental findings reveal that the overall execution times for polynomial degrees 26, 28, and 210 are 2.2 ms, 4.4 ms, and 25 ms, respectively. The solution is beneficial for large data security applications such as environmental, financial, and healthcare data analytics.

Daun Jung et al. [8] first configured a nuclear power plant protection system environment for the nuclear reactor APR1400, after which the threat assessment results were compared and analyzed based on the allocation of security controls in cases where only NEI 13-10 was used, as well as when it was used in conjunction with TAM. When just NEI 13-10 is used, the threat assessment findings show that there are limitations to minimizing all hazards. However, when used in conjunction with TAM, all risks (including those that could not be identified previously) may be mitigated by using TAM's five important benefits, allowing them to overcome the restrictions of NEI 13-10 and mitigate threats more effectively. Yun Guo et al. [9] examine the cyber security risks and countermeasures faced by physical protection systems of Nuclear Power Plants. They propose the concept of developing a cyber security test platform for physical protection systems based on digital twin technology, and investigate relevant key technologies, providing a new perspective for the cyber security protection of physical protection systems in nuclear power plants around the world.

Seungmin Kim et al. [10] suggested criteria for selecting VDAs (Vital Digital Assets) of a Nuclear Power Plant and included examples to assist readers understand the process. They gathered the information for selecting VDAs, identifying beginning events that can be produced by cyber-attacks, selecting and analyzing accident mitigation facilities, and picking VDAs from target sets are the procedures for selecting VDAs. To protect the nuclear power plant from cyber-attacks, digital assets are classified and managed as critical digital assets which have safety, security, and emergency preparedness functions.

Jae Hee Roh et al. [11] presented a cyber security system that may be employed in control networks that demand high levels of reliability, such as nuclear power plants. DACS (Detection on Attacking Control System), DACS management program (DMP) to centrally administer numerous DACS, and central monitoring system (CMS) to store system logs comprise the proposed system. DACS's packet detection function is handled by a real-time packet detector written in FPGA that handles a 7-tuple whitelist of the source and destination network nodes' MAC address, IP address, protocol, and TCP/UDP port number. This study demonstrated the utility of the proposed system by offering an example of its application to the nuclear power plant safety system.

Ruba Awadallah et al. [12] provide a brief overview of cloud computing security challenges and demonstrate that Homomorphic Encryption alone is unable to produce indistinguishable ciphertext in the face of adaptive chosen-ciphertext attacks. The study finishes by offering various solutions to the highlighted problem.

Nikolay N. Kucherov et al. [13] provide an overview and comparison of existing homomorphic encryption algorithms for machine learning tasks. The use of homomorphic ciphers enables the processing of encrypted data while protecting the data's privacy. Homomorphic encryption is being actively employed in machine learning activities to transport and protect the secrecy of resource-intensive processes for cloud-based neural network training.

Zainab Hikmat Mahmood et al. [14] provide an overview of cloud computing security challenges, they also stated that the use of the fully homomorphic encryption technology has limitations such as big key size and low computation efficiency, making it unsuitable for safe cloud computing. They devise a hybrid homomorphic encryption technique based on the additively (single-bit) homomorphic GM encryption algorithm and the multiplicative homomorphic RSA algorithm. The hybridization of homomorphic encryption systems appears to be a viable method of circumventing their constraints while benefiting from their resilience to confidentiality assaults. This hybridization of homomorphic encryption algorithms increased the speed 2.9 times, reduced the computing time to 66 ms. Nayna Jain et al. [15] address the computational complexity in a convolutional deep neural network for encrypted processing. In this paper, they perform encrypted inference experiments on the MNIST dataset using the CKKS encryption technique from the open-source HELib package. The studies show that effective ciphertext packing approaches, model optimization, and multi-threading tactics are

crucial in deciding the inference process's throughput and latency. They also show that operational parameters of the chosen FHE scheme, such as the degree of the cyclotomic polynomial, depth limitations of the underlying leveled HE scheme, and computational precision parameters, result in significant tradeoffs between the machine learning model's accuracy, security level, and computational time. The paper's main contribution is the examination and proposal of optimization approaches for efficient encrypted CNN inference. Sonal Mittal et al. [16] examined many forms of FHE schemes, such as integer and polynomial over the ring of integer systems. The paper also contains the fundamental procedures required to build any FHE scheme. The programs are discussed, together with their benefits and drawbacks. A total of four FHE schemes were reviewed in this study, with an emphasis on two alternative symmetric FHE schemes based on integers (DGHV) and polynomial rings over integers suggested by Dasgupta and Pal.

Aleksey Poletykin et al. [17] investigated the issue of cybersecurity risk assessment for critical facility process control systems (APCS). The internal and external contexts of risk assessment are examined using the example of APCS for NPP. For the development life cycle stage and the APCS operating stage, two methodologies are provided. The research also examines challenges with the process of controlling APCS cybersecurity for NPP at various phases of the life cycle. The practical challenges of risk assessment at the design and operation stages of APCS for NPP are also provided.

Alexander Viand et al. [18] studied, assessed, and Systematized FHE tools and compilers in this paper. The proliferation of sensitive data in cloud services and a rash of data breaches has prompted highly regulated enterprises to seek more secret and secure computing solutions. As a result of this need, there has been a recent increase in the creation of FHE tools. They undertake an exhaustive survey and experimental review to study the present state of the art and propose areas for future improvement to grasp the landscape of recent FHE tool advances. They conducted trials to assess the performance and usefulness of these technologies in several applications. They conclude with tips for developers planning to create FHE-based apps and a discussion of potential FHE tool development paths.

[19] The paper acknowledges that SMRs and advanced nuclear reactors have gained attention as potential alternatives to traditional large-scale nuclear reactors. These newer designs aim to offer advantages such as enhanced safety, scalability, flexibility, and lower costs. However, the

paper emphasizes the importance of critically assessing the claims and realities associated with these technologies. It discusses several earlier studies and experiences, highlighting limitations and challenges. The paper points out that the high costs associated with SMRs and advanced reactors have been a significant challenge. The earlier work in this area has highlighted the uncertainties and difficulties in accurately estimating the costs of these advanced designs. Many projects have experienced significant cost overruns and delays, leading to financial challenges. The paper emphasizes the need for comprehensive and realistic cost assessments to avoid unrealistic expectations and financial risks.

Earlier studies have also highlighted safety and regulatory challenges associated with SMRs and advanced reactors. These designs often incorporate new technologies and materials, which may require additional regulatory scrutiny. The paper discusses concerns related to the licensing process, regulatory frameworks, and public acceptance. It emphasizes the importance of robust safety assessments, addressing potential vulnerabilities, and ensuring effective regulatory oversight. The issue of radioactive waste management is another area of concern. The paper discusses earlier studies that have raised questions about the feasibility and long-term sustainability of waste management strategies for SMRs and advanced reactors. It highlights the challenges associated with waste disposal, the potential for proliferation of nuclear materials, and the need for robust safeguards and non-proliferation measures.

Earlier work has also highlighted technical feasibility challenges with SMRs and advanced reactors. The paper mentions studies that have identified technical uncertainties and operational challenges associated with these designs. Examples include issues related to materials, fuel performance, cooling systems, and long-term operational reliability.

While the paper does not explicitly discuss FHE or encryption-related technologies, it offers a comprehensive review of the earlier work and limitations in the area of small modular and advanced nuclear reactors. It highlights the importance of critically evaluating claims and addressing challenges in various aspects, including cost, safety, waste management, and technical feasibility. Understanding these limitations and addressing them effectively is crucial for the successful development and deployment of advanced nuclear reactor technologies, including potential future applications of encryption technologies like FHE in the nuclear power industry.

[20] The paper acknowledges the increasing importance of cyber security in the context of nuclear power plants, as they are critical infrastructure assets. It discusses earlier research and studies that have addressed the challenges and approaches in this domain.

Earlier work has highlighted the evolving threat landscape and the vulnerabilities faced by nuclear power plants in terms of cyber attacks. The paper discusses studies that have analyzed different types of cyber threats, including state-sponsored attacks, hacktivism, and insider threats. It emphasizes the importance of understanding the potential consequences of successful cyber attacks on nuclear power plants and the need for robust security measures.

The paper explores earlier research on risk assessment methodologies for cyber security in nuclear power plants. It discusses studies that have proposed frameworks and approaches to assess the risks associated with cyber attacks. These methodologies consider various factors such as asset criticality, threat likelihood, and vulnerability severity to prioritize security measures. The paper highlights the importance of risk assessment in determining the appropriate cyber security measures for nuclear power plants.

Earlier studies have emphasized the importance of adopting a defense-in-depth approach to cyber security in nuclear power plants. This approach involves implementing multiple layers of security controls to protect critical assets. The paper discusses research that has proposed various security measures, including network segmentation, intrusion detection systems, access controls, and incident response plans. It emphasizes the need for a holistic and comprehensive security strategy.

Earlier work has also highlighted limitations and challenges in ensuring cyber security in nuclear power plants. The paper mentions studies that have identified issues such as legacy systems, human factors, supply chain vulnerabilities, and the rapid evolution of cyber threats. These limitations pose challenges in implementing robust security measures and require continuous monitoring and adaptation.

Overall, the paper provides insights into the earlier work done in the area of cyber security in nuclear power plants. It discusses the evolving threat landscape, risk assessment methodologies, defense-in-depth approaches, and the limitations and challenges associated with ensuring cyber security. While FHE is not specifically addressed in the paper, it is worth noting that encryption technologies, including FHE, can play a role in enhancing the security of sensitive data and communication within nuclear power plants. Future research may explore the potential application of FHE and other encryption techniques in strengthening the cyber

security posture of nuclear power plants.

[21] The paper acknowledges the importance of cyber security in nuclear power plants and highlights the evolving threat landscape in the context of cyber attacks. It also discusses earlier research and studies that have addressed cyber security in nuclear power plants, particularly focusing on intrusion detection systems (IDS). Here are some key points:

Earlier work has explored various approaches and techniques for intrusion detection in nuclear power plants. This includes signature-based detection, anomaly-based detection, and hybrid approaches. The paper discusses previous research that has proposed different IDS architectures and algorithms to detect and prevent cyber attacks on critical systems. These IDS solutions aim to identify malicious activities, abnormal behaviors, and potential vulnerabilities in the network infrastructure of nuclear power plants.

The paper specifically focuses on the use of FPGA technology for implementing the network intrusion detection system in nuclear power plants. FPGA offers advantages such as high performance, low latency, and reconfigurability, which are crucial for real-time monitoring and response in critical environments. The earlier work has explored the use of FPGA in various security applications, including intrusion detection, to improve the detection speed and accuracy of cyber threats.

Earlier research has highlighted several limitations and challenges in implementing cyber security systems, including intrusion detection, in nuclear power plants. These challenges include the complexity of the operational environment, the diversity of networked systems, the need for continuous monitoring, the high volume of network traffic, and the dynamic nature of cyber threats. The paper emphasizes the importance of addressing these challenges and provides insights into the approach taken in their research to overcome these limitations.

The approach presented in the paper involves the development of an FPGA-based network intrusion detection system specifically tailored for the unique requirements of nuclear power plants. The authors propose a hybrid IDS architecture that combines signature-based and anomaly-based detection techniques. They utilize the high-speed processing capabilities of FPGA to analyze network traffic in real-time and identify potential cyber threats. The paper describes the design, implementation, and performance evaluation of the FPGA-based IDS, highlighting its effectiveness in detecting various types of attacks.

In summary, the paper contributes to the earlier work in the area of cyber security in nuclear power plants by focusing on the development of an FPGA-based network intrusion detection system. It discusses earlier research on intrusion detection systems, the use of FPGA technology, and the challenges associated with ensuring cyber security in nuclear power plants. By leveraging the advantages of FPGA, the research presented in the paper aims to enhance the security posture of nuclear power plants and strengthen their ability to detect and prevent cyber attacks.

[22] The paper acknowledges the importance of assessing the effectiveness of security systems in nuclear facilities, particularly in the context of cyber-physical attacks. It discusses earlier research and studies that have addressed the evaluation of security systems in nuclear facilities and the challenges associated with such evaluations.

Earlier work has focused on evaluating the performance and effectiveness of security systems deployed in nuclear facilities. This includes assessing the detection capabilities, response time, alarm generation, and overall system robustness. The paper discusses previous research that has proposed evaluation methodologies, metrics, and scenarios to simulate realistic attack scenarios and measure the performance of security systems. These evaluations aim to identify vulnerabilities, gaps, and areas for improvement in the security infrastructure of nuclear facilities.

The paper specifically considers the evaluation of security systems under cyber-physical attack scenarios. Cyber-physical attacks involve exploiting vulnerabilities in both the cyber (information technology) and physical (control systems) domains to compromise the security and operations of nuclear facilities. Earlier research has explored various cyber-physical attack vectors and their potential impacts on nuclear facilities. The paper discusses the importance of assessing the effectiveness of security systems in mitigating cyber-physical threats and the challenges associated with such evaluations.

Earlier research has identified limitations and challenges in evaluating the effectiveness of security systems in nuclear facilities. These include the complexity and heterogeneity of the security infrastructure, the interdependencies between cyber and physical systems, the dynamic nature of cyber threats, and the need for realistic and comprehensive evaluation scenarios. The paper emphasizes the importance of addressing these limitations and provides insights into the approach taken in their research to overcome these challenges.

The approach presented in the paper involves the development of an evaluation framework to assess the effectiveness of a security system in a nuclear facility under a cyber-physical attack scenario. The authors simulate a realistic attack scenario, considering both cyber and physical components, to evaluate the system's response capabilities, alarm generation, and overall effectiveness in mitigating the attack. The paper describes the evaluation methodology, metrics, and simulation results, highlighting the strengths and limitations of the security system under assessment.

In summary, the paper contributes to the earlier work in the area of evaluating security systems in nuclear facilities under cyber-physical attack scenarios. It discusses earlier research on the evaluation of security systems, the consideration of cyber-physical attack scenarios, and the challenges associated with such evaluations. By developing an evaluation framework and simulating realistic attack scenarios, the research presented in the paper aims to enhance the understanding of the vulnerabilities and effectiveness of security systems in nuclear facilities. This knowledge can help identify improvements and strengthen the security infrastructure to mitigate cyber-physical threats effectively.

[23] The paper acknowledges the significance of cyber security in nuclear power plants, particularly in relation to the physical protection systems. It discusses earlier research and studies that have addressed cyber security risk analysis and the use of digital twin technology in this context.

Earlier work has focused on conducting risk analysis for cyber security in nuclear power plants. This includes identifying vulnerabilities, threats, and potential consequences of cyber attacks on physical protection systems. The paper discusses previous research that has proposed methodologies, models, and frameworks to assess the cyber security risks associated with physical protection systems. These risk analyses aim to identify weaknesses, prioritize security measures, and enhance the resilience of nuclear power plants against cyber threats.

The paper explores the use of digital twin technology as a means to create a cyber security test platform for nuclear power plants. Digital twin refers to a virtual replica or simulation of a physical system, which can be used for various purposes, including testing and analysis. Earlier research has investigated the application of digital twin technology in different domains, including cyber security. The paper discusses how digital twin technology can be leveraged to



simulate cyber attacks, test security measures, and evaluate the effectiveness of physical protection systems in detecting and mitigating cyber threats.

Earlier research has identified limitations and challenges in conducting cyber security risk analysis and implementing digital twin technology in nuclear power plants. These include the complexity of the physical protection systems, the evolving nature of cyber threats, the need for accurate modeling and simulation, the availability of data and information for analysis, and the integration of cyber security measures into existing systems. The paper emphasizes the importance of addressing these limitations and provides insights into the approach taken in their research to overcome these challenges.

The approach presented in the paper involves the development of a cyber security test platform using digital twin technology. The authors create a virtual model of the physical protection systems in a nuclear power plant, incorporating various components and their interactions. They simulate cyber attacks on the digital twin to evaluate the vulnerabilities and effectiveness of security measures. The paper describes the methodology, implementation details, and the results obtained from the cyber security risk analysis conducted on the digital twin platform.

In summary, the paper contributes to the earlier work in the area of cyber security risk analysis of physical protection systems in nuclear power plants. It discusses earlier research on cyber security risk analysis, the application of digital twin technology, and the limitations and challenges associated with these areas. By utilizing digital twin technology, the research presented in the paper aims to enhance the understanding of cyber security risks, test security measures, and improve the resilience of physical protection systems in nuclear power plants against cyber threats.

[24] The paper acknowledges the importance of fully homomorphic encryption in cloud computing, where sensitive data needs to be processed while maintaining its confidentiality. It discusses earlier research and studies that have focused on developing FHE schemes and highlights the limitations of those schemes. Here are some key points:

Earlier work in the field of fully homomorphic encryption has proposed various schemes to enable computation on encrypted data. These schemes include the original FHE scheme proposed by Gentry and subsequent advancements in the field. The paper discusses the

limitations of earlier FHE schemes, such as high computational overhead, large ciphertext expansion, and limited support for certain types of operations. These limitations have hindered the practical adoption of FHE in real-world scenarios, including cloud computing.

The paper presents a new approach that utilizes multistage partial homomorphic encryption as the basis for the fully homomorphic encryption scheme. This approach aims to overcome the limitations of earlier FHE schemes by addressing the computational overhead and ciphertext expansion issues. The multistage technique allows for dividing the computation into multiple stages, each utilizing partial homomorphic encryption, thus reducing the overall computational complexity. The paper describes the construction and properties of the proposed scheme, highlighting its advantages over earlier FHE schemes.

Earlier research has identified several limitations and challenges in the field of fully homomorphic encryption. These include the high computational requirements for performing homomorphic operations, the ciphertext expansion leading to increased storage and communication overhead, the limited support for certain types of computations, and the need for secure key management. The paper emphasizes the importance of addressing these limitations and provides insights into the approach taken in their research to overcome these challenges.

The approach presented in the paper involves the development of a new fully homomorphic encryption scheme based on multistage partial homomorphic encryption. The authors propose a construction that combines different stages of partial homomorphic encryption to enable computation on encrypted data while minimizing the computational complexity and ciphertext expansion. The paper provides mathematical formulations, security analysis, and performance evaluations of the proposed scheme, demonstrating its effectiveness in achieving fully homomorphic encryption with improved efficiency.

In summary, the paper contributes to the earlier work in the field of fully homomorphic encryption by proposing a new scheme based on multistage partial homomorphic encryption. It discusses earlier FHE schemes, their limitations, and the challenges associated with achieving practical fully homomorphic encryption. By addressing the limitations through the multistage approach, the research presented in the paper aims to advance the adoption of fully homomorphic encryption in cloud computing and overcome the computational and efficiency

challenges of earlier schemes.

[25] The paper acknowledges the criticality of cyber security in nuclear power plants and the need for an effective strategy to protect vital digital assets. It discusses earlier research and studies that have addressed cyber security in the context of nuclear power plants, with a focus on protecting key digital assets.

Earlier work has explored various approaches to enhance cyber security in nuclear power plants. This includes the development of security frameworks, risk assessment methodologies, intrusion detection systems, and incident response procedures. The paper discusses previous research that has proposed different strategies to protect critical assets and systems, including digital assets, from cyber threats. These approaches aim to identify vulnerabilities, prioritize security measures, and enhance the resilience of nuclear power plants against cyber attacks.

The paper specifically focuses on the concept of vital digital assets and their significance in cyber security strategy. Vital digital assets refer to the essential digital components or systems that are crucial for the safe and secure operation of nuclear power plants. Earlier research has recognized the importance of identifying, protecting, and monitoring these assets to ensure the integrity and reliability of nuclear power plant operations. The paper discusses the approach of considering vital digital assets as a central element in developing a cyber security strategy.

Earlier research has identified limitations and challenges in implementing effective cyber security strategies in nuclear power plants. These include the evolving nature of cyber threats, the complexity and diversity of digital systems, the need for continuous monitoring and threat intelligence, the integration of cyber security into existing processes, and the coordination between various stakeholders involved in nuclear power plant operations. The paper emphasizes the importance of addressing these limitations and provides insights into the approach taken in their research to overcome these challenges.

The approach presented in the paper involves the development of a comprehensive cyber security strategy for nuclear power plants using vital digital assets. The authors propose a framework that encompasses key elements such as risk assessment, threat intelligence, access control, monitoring, incident response, and training. The strategy focuses on identifying and protecting vital digital assets, implementing proactive measures to prevent cyber attacks, and establishing robust incident response procedures. The paper describes the framework, its

components, and their interrelationships, highlighting its effectiveness in enhancing cyber security in nuclear power plants.

In summary, the paper contributes to the earlier work in the area of cyber security in nuclear power plants by proposing a comprehensive strategy using vital digital assets. It discusses earlier research on cyber security approaches, the concept of vital digital assets, and the limitations and challenges associated with implementing effective cyber security strategies. By emphasizing the importance of protecting vital digital assets and providing a comprehensive framework, the research presented in the paper aims to enhance the cyber security posture of nuclear power plants and mitigate the risks associated with cyber threats.

# Chapter 3

## PROBLEM STATEMENT

Nuclear power plants handle critical and sensitive information related to the operation, control, and safety of the facility. Protecting the confidentiality and privacy of this data is of utmost importance to ensure the security and integrity of the plant's operations[21]. Fully Homomorphic Encryption (FHE) presents an intriguing solution that allows computations to be performed on encrypted data, maintaining the confidentiality of the sensitive information while enabling secure data processing.

### 3.1 Project Objectives:

- **Create a Robust Integration Framework with Monte Carlo Methods:** The main goal is to build and create a robust integration framework with Monte Carlo methods for carrying out precise and trustworthy integration computations. To maintain data privacy and security throughout the computation process, the framework should smoothly integrate FHE capabilities using Ziroh Lab's FHE libraries.
- **Enable computations on encrypted data while protecting the privacy and confidentiality of sensitive data,** such as decay constants and operational variables, by implementing FHE. Utilising FHE to perform integration calculations securely is the goal in order to prevent unauthorised access to or exposure of important operational data.
- **Assess Accuracy and Performance:** Carry out a thorough assessment of the Monte Carlo integration approach's accuracy and performance. To evaluate the accuracy attained while taking into account the computational overhead provided by FHE, compare the results from FHE-based Monte Carlo integration computations with those from conventional non-encrypted methods. The goal is to show that performance constraints can be met while FHE-based Monte Carlo integration can deliver results with acceptable accuracy.
- **Ensure Seamless Integration and Compatibility:** Make that the FHE-based Monte Carlo integration framework is compatible with the infrastructure, databases, and other

systems already in place in nuclear power plants. This goal entails dealing with compatibility issues, making sure that data exchange is effective, and preserving the integrity of the integrated system. In order to make the implementation of FHE-based integration calculations easier, the objective is to develop a comprehensive and compatible integration solution that smoothly integrates into the current operational environment.

### 3.2 Project Assumptions:

- The project presupposes the availability of sufficient computing resources that can handle the computational needs of FHE-based integration computations performed using Monte Carlo techniques. This includes having access to high-performance servers or cloud infrastructure with enough RAM and CPU to support the calculation and encryption procedures.
- Effectiveness and Dependability of Ziroh Lab's FHE Libraries: The project makes the assumption that Ziroh Lab's FHE libraries offer a dependable and effective foundation for putting FHE methods into practise. It is assumed that the libraries provide the required features, algorithms, and support for smooth integration with Monte Carlo techniques, ensuring precise and secure integration calculations within the context of nuclear power plants.
- The initiative is based on the supposition that all applicable security and privacy laws governing the management of sensitive data in nuclear power plants are complied with. It is assumed that the FHE implementation and Monte Carlo integration computations abide by industry-specific security norms and legal specifications, protecting sensitive data and preserving data privacy.
- Adequate Training and Knowledge of FHE and Monte Carlo Methods: The project presupposes that the project team is knowledgeable and skilled in FHE, Monte Carlo techniques, and the FHE libraries from Ziroh Lab. It is based on the supposition that the team members have received the necessary training or have the necessary skills to comprehend the fundamental ideas, put the integration framework into practise, and utilise the FHE capabilities in a secure and accurate manner.

### 3.3 Challenges And Considerations

- **Computational Complexity:** FHE schemes are known to be computationally intensive. The operations on encrypted data require additional computational resources, which can result in increased processing time and resource utilization. In the context of nuclear power plants, where real-time operations and decision-making are crucial, the computational overhead introduced by FHE needs to be carefully managed. Efficient implementation strategies, hardware acceleration, or cloud-based computing resources can be explored to mitigate the impact of computational complexity.
- **Performance Impact:** FHE exhibits ciphertext expansion, where the size of the encrypted data grows with each computation. In nuclear power plants, which handle large volumes of data from various sensors and monitoring systems, the increased storage requirements can become a challenge. It may necessitate optimizing data storage techniques, employing data compression algorithms, or considering efficient data transfer mechanisms to maintain the required performance and minimize the impact on data transmission speed.
- **Real-Time Data Analysis:** Nuclear power plants continuously monitor and analyze data from numerous sensors and systems to ensure safe and efficient operation. Real-time analysis is vital for timely detection of anomalies and rapid response to any potential issues. Integrating FHE into real-time data analysis processes requires careful consideration of the computational time required for performing computations on encrypted data. Optimization techniques, parallel processing, or dedicated hardware acceleration can be explored to ensure that FHE computations can be performed within the necessary time constraints.
- **Key Management:** FHE relies on encryption keys for secure operations. Robust key management practices are crucial in the context of nuclear power plants to safeguard the encryption keys, prevent unauthorized access, and ensure the integrity of the encryption process. Key generation, distribution, rotation, and storage mechanisms should adhere to industry best practices and regulatory requirements to maintain the

highest level of security.

- **Regulatory Compliance:** Nuclear power plants operate within a regulatory framework that imposes strict requirements for data security, privacy, and operational integrity. Any encryption technique, including FHE, must comply with these regulations. The implementation of FHE should align with relevant industry standards, security certifications, and data protection regulations to ensure legal compliance and maintain the trust of regulatory authorities.
- **Integration with Legacy Systems:** Nuclear power plants often rely on legacy systems and infrastructure that may not be compatible with modern encryption techniques like FHE. Integration challenges may arise when attempting to incorporate FHE into existing systems, protocols, or data formats. It is essential to assess the compatibility of FHE with legacy systems, considering data formats, communication protocols, and potential software or hardware upgrades required for seamless integration.

By addressing these challenges and considerations, nuclear power plants can harness the benefits of FHE to protect sensitive data, ensure secure computations, and enhance the overall security posture of their operations. Thorough evaluation, proper planning, and collaboration with experts in cryptography and security can contribute to successful implementation and adoption of FHE within the nuclear power industry.

Fully Homomorphic Encryption (FHE) has emerged as a possible answer to the growing need for safe and privacy-preserving data processing. FHE can provide a safe and effective method for carrying out integration calculations while maintaining data confidentiality in the setting of nuclear power plants, where sensitive operational data needs to be preserved. In particular, this study employs the FHE libraries from Ziroh Lab to build FHE for integration computations in nuclear power plants. The objective is to investigate the viability and advantages of adopting FHE in this area, with a focus on safeguarding private data and maintaining the accuracy of integration computations.



### 3.4 Project Limitations:

Implementing Fully Homomorphic Encryption (FHE) for integration calculations in nuclear power plants using Ziroh Lab's FHE libraries has many advantages. However, it is important to be aware of the limitations that may affect the project. Some of the key limitations include:

- **Computational overhead:** FHE computations typically require more computational resources and take longer to process than traditional non-encrypted calculations. This additional overhead can impact the overall performance of the system, potentially causing delays in obtaining integration results.
- **Scalability challenges:** FHE schemes, especially in complex scenarios involving large datasets or intricate mathematical operations, may face scalability challenges. As the size and complexity of the integration calculations increase, the computational demands of FHE may become more significant, making it crucial to assess the scalability of the proposed architecture.
- **Integration complexity:** Integrating FHE into existing systems within nuclear power plants can be a complex task. Ensuring compatibility, adaptability, and efficient integration with other operational systems, databases, or infrastructure components may require substantial effort and coordination with various stakeholders.
- **Learning curve and expertise:** Effectively implementing FHE and utilizing Ziroh Lab's FHE libraries require a certain level of expertise and familiarity with the underlying concepts of FHE. Adequate training and skill development may be necessary for the project team to fully understand and utilize the capabilities of FHE and the specific features provided by Ziroh Lab's libraries.
- **Security considerations:** While FHE offers strong security guarantees, it is crucial to maintain a holistic approach to security. The implementation should consider other security aspects, such as key management, secure communication channels, and protection against potential side-channel attacks, to ensure the overall security of the system.
- **Regulatory compliance:** The introduction of FHE into nuclear power plant operations may require compliance with industry-specific regulations and standards. Careful consideration must be given to ensure that the implemented solution meets the necessary regulatory requirements and maintains compliance throughout the project.

lifecycle.

- **Cost implications:** The adoption of FHE and integration with Ziroh Lab's FHE libraries may involve financial costs, including licensing fees, infrastructure upgrades, and training expenses. A thorough cost-benefit analysis should be conducted to assess the feasibility and cost-effectiveness of implementing FHE for integration calculations in nuclear power plants.

It is important to recognize these limitations and address them effectively to ensure the successful implementation of FHE for integration calculations in nuclear power plants. By carefully managing these constraints, the project can maximize the benefits of FHE while mitigating potential challenges and risks.

# Chapter 4

## PROJECT REQUIREMENTS

The project specifications for Fully Homomorphic Encryption (FHE) implementation using Ziroh Lab's FHE libraries for integration calculations in nuclear power plants include a thorough methodology to assure the successful integration of FHE in this crucial domain. The main goal is to use Ziroh Lab's libraries and FHE algorithms to execute integration calculations while protecting the security and privacy of important operational data. The concept involves conducting integration calculations directly on the encrypted data after encrypting crucial variables, including decay constants, using FHE. For proper integration results, the output of these computations will be decrypted.

### 4.1. Human Resources:

1. Java Developers:
  - Skilled personnel proficient in Java programming language
  - Experienced in secure coding practices.
  - Familiar with nuclear power plant systems and software development
2. Cryptography Experts:
  - Experts in cryptographic protocols and algorithms
  - Capable of guiding secure implementation of FHE in Java
  - Ensuring confidentiality and integrity of sensitive data

### 4.2. Reusable Software Components:

1. Java Cryptography Architecture (JCA):
  - Standardized Java libraries and APIs for cryptographic operations
  - Seamless integration of FHE encryption and decryption functions
2. FHE Libraries:
  - Prebuilt Java libraries implementing FHE protocols and algorithms
  - Optimized functions for encrypted data processing
  - Reducing development effort and ensuring reliable encryption operations

**4.3. Software & Hardware Requirements:**

- Java Development Environment:
- Integrated Development Environments (IDEs) like Eclipse or IntelliJ IDEA
- Efficient coding, debugging, and testing of FHE integration in Java

**4.4. Other Requirements**

- Interoperability with Existing Java Applications:
- Compatibility and seamless integration with the plant's existing Java-based systems and software applications
- Leveraging shared libraries and APIs for efficient communication and data exchange

# Chapter 5

## SYSTEM DESIGN PROPOSED ARCHITECTURE

The architecture includes a multi-layered design with processes for encryption and decryption, computations on encrypted data integration, and appropriate interfaces for easy integration with current systems. This introduction gives a general overview of the system architecture and major elements, emphasising the value of using FHE and the FHE libraries from Ziroh Lab to address privacy and security issues in nuclear power plant operations while carrying out integration calculations.

### 5.1. Hardware Requirements:

- High-performance servers or systems capable of running the homomorphic encryption algorithms with minimal latency and maximum throughput.
- Sufficient storage capacity to store encrypted and decrypted data.
- Robust network infrastructure to ensure secure and reliable data transmission.

### 5.2. Software Requirements:

- Operating system: Windows 11
- Homomorphic encryption libraries: Ziroh Labs homomorphic encryption libraries
- Programming language: Java and Python
- Development tools: IDEs such as IntelliJ or Eclipse, version control systems such as Git or SVN, and code review tools such as Gerrit or Crucible.

## 5.3 UML Diagrams

### 5.3.1 Use case Diagram



Fig 5.1. Use Case Diagram

### 5.3.2. Activity Diagram

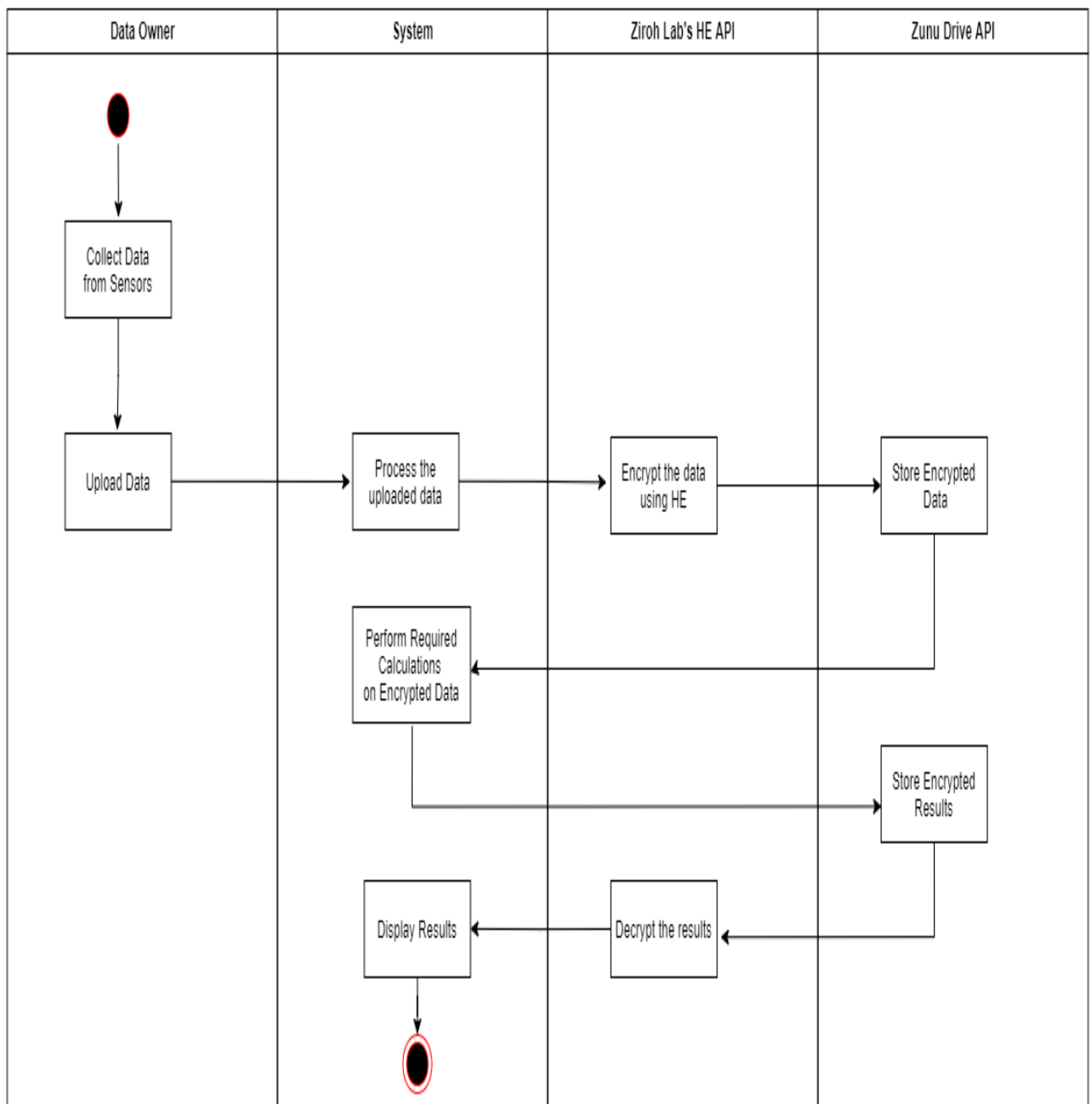


Fig 5.2. Activity Diagram

### 5.3.3. Class Diagram

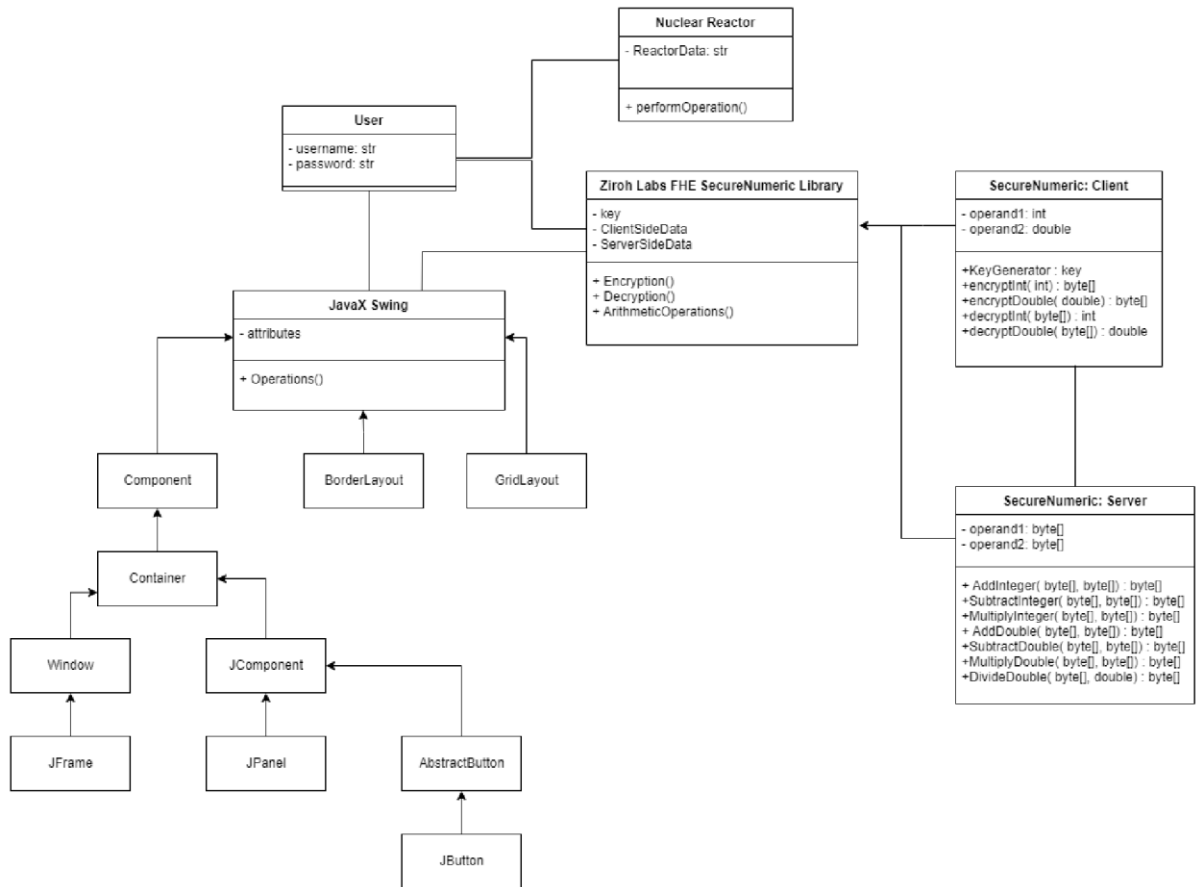


Fig 5.3. Class Diagram



# Chapter 6

## PROJECT PLAN

Duration: January 2023 to May 2023

### 6.1. Project Initiation Phase (January 2023):

- Establish the goals, scope, and deliverables of the project.
- Create a project team and assign roles and duties accordingly.
- Develop project governance and develop communication channels.
- Perform preliminary analysis on FHE, integration computations, and the FHE libraries from Ziroh Lab.

### 6.2. Requirements Gathering and Analysis (January to February 2023):

- Engage stakeholders to learn about the needs for integration calculations in nuclear power plants.
- The requirements' functional and non-functional documentation.
- Decide on the required data inputs, integration techniques, and desired graphical results.
- To determine whether FHE, IntelliJ, Eclipse, Java Swing, and Google Collab ( Python ) are appropriate for the project, conduct a feasibility study.

### 6.3. Design and Development Phase (February to April 2023):

- Create the system architecture overall, incorporating JavaSwing, FHE, IntelliJ, Eclipse, and Google Colab Python.
- Utilise the FHE libraries from Ziroh Lab to create the modules for encryption and decryption.
- Utilise the features of IntelliJ and Eclipse as development platforms to implement integration calculations using Monte Carlo techniques.
- Create a user-friendly GUI for input and output visualisation by integrating Java Swing.
- Use Google Colab Python to create and analyse graphs.

### 6.4. Testing and Quality Assurance (April 2023):

- To validate the precision and validity of integration computations, use unit testing.
- Conduct system testing to confirm the integrated solution's overall functionality.
- Conduct security testing to evaluate the FHE and encryption modules' abilities to protect user privacy.
- Any problems, errors, or performance bottlenecks found during testing should be fixed.

### **6.5. Documentation and Finalization (April to May 2023):**

- Perform a project review to determine the successes, difficulties, and lessons learned.
- Give an overview of the project's results, including the integrated FHE solution for nuclear power reactors' integration calculations.
- Get input from the relevant parties, then resolve any remaining issues or suggestions.
- Save project files and products in the archives.

It should be noted that the project plan is only a high-level blueprint and may need to be further customised and detailed depending on the individual project requirements, resource availability, and stakeholder involvement.

# Chapter 7

## METHODOLOGY

Our methodology follows the idea of applying integration on simple equations which have relevance in the working of a nuclear power plant. We have used the idea of calculating decay factor and decay constant in a hypothetical scenario which is explained below.

### 7.1. Proposed Work

In nuclear power plants, radioactive elements are subject to a decay process in which they are converted into daughter elements through the emission of particles or radiation. This transformation is determined by the decay constant, which indicates the probability with which a radioactive atom decays per unit time. As the parent element decays and creates daughter elements, the concentration of the parent element decreases, causing the decay constant to change over time. This change in the decay constant directly affects the decay curve, or graph, that depicts the decay of the radioactive element. The decay curve initially shows a rapid drop in the concentration of the parent element, indicating a high decay constant. However, as time progresses and the concentration of parent element decreases, the decay constant decreases, resulting in a slower rate of decay and a more gradual increase in the decay curve. The production of daughter elements in nuclear power plants is a fundamental process that affects the decay constant and the plot of radioactive decay. With this in mind, we propose how Integration can be performed in FHE, especially in the above stated situation with a few scenarios.

Consider a situation where a nuclear power plant uses a variety of radioactive components to operate. The specific decay constant for each element controls how fast it decays. However, the decay constant of a particular element can change over time due to operational changes or fluctuations in fuel composition. The slope and shape of the decay plot may change due to this variation. Such dynamic situations can be effectively analysed and monitored using time integration. By integrating the measured decay rates over specified periods

of time, it is possible to gain a deeper understanding of the overall decay behaviour. This method takes into account fluctuations in the decay constant and provides important information about the use and functioning of the radioactive element in the power plant. An indicator of the presence of an element is the decay constant associated with that element. It is possible to determine the type of radioactive element used in a nuclear power plant by examining the decay constant. However, for reasons of privacy, it can be advantageous to hide the decay constant. A decay constant of radioactive elements could potentially reveal private information about the type and composition of the fuel used, which could have security implications or reveal details about confidential technology.

Therefore, protecting the decay constant as secret information helps maintain the security and privacy of nuclear power plant operations by preventing unauthorized access to or misuse of such information by criminals.

Therefore, in our proposed work, we use FHE to encrypt the decay constant and have integration performed on calculating the decay factor. Every step involved is encrypted with no decryption happening at anything stage. There are three scenarios with variations in simple integration equations which we have stated below.

The very first scenario to consider would be one in which we have a specific decay constant of a single element. The amount of the element would vary depending upon the decay factor which is given by the following formula:

$$e^{-\lambda t} \quad (1)$$

Here,  $\lambda$  is the decay constant and 't' is the time over which we want to find the amount of element decayed.

The remaining nuclei fraction equal to the decay factor:

$$\frac{N(t)}{N(0)} = e^{-\lambda t} \quad (2)$$

$N(t)$  is the amount of nuclei after decaying and  $N(0)$  is the amount of nuclei at the beginning.

This can be further written as:

$$\int \frac{N(t)}{N(0)} dN(t) = \int e^{-\lambda t} \cdot dt \quad (3)$$

$$\ln \left( \frac{N(t)}{N(0)} \right) = -\int \lambda t \cdot dt \quad (4)$$

Considering the above equation, we are able to calculate the log of fraction of remaining nuclei

by using:

$$-\int \lambda t \cdot dt \quad (5)$$

## 7.2. Scenarios And Algorithms

### 7.2.1. Scenario Of Simple Integration:

If the decay constant does not change as we are only considering a single element in the scenario, we could integrate the following over time:

$$-\lambda \int t \cdot dt \quad (6)$$

Here is the algorithm for calculating the simple integral of  $t \cdot dt$  using Monte Carlo approximation:

**Algorithm 1** Algorithm to calculate simple integration of  $t \cdot dt$  using Monte Carlo Approximation

- 0: Read the number of iterations from command-line argument
- 1: Define the range of integration
- 2: Initialize variables
- 3: Create a random number generator 4: Perform Monte Carlo approximation 5: for 0 to tier do
- 6: Generate a random value in the range [0, 60]
- 7: Scale the random value to the range of integration
- 8: Evaluate the function  $t$  and add it to the sum
- 9: Calculate the approximate integral
- 10: Print the result

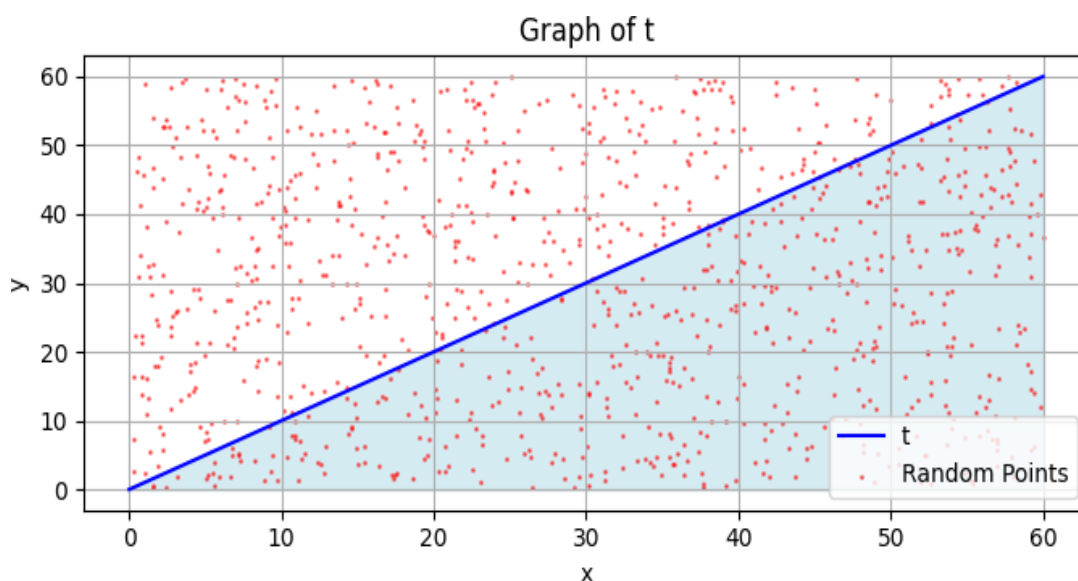


Fig 6.1. Graph of simple single variable curve using Monte Carlo integration

### 7.2.2. Scenario Of Polynomial Integration

To consider a more complex equation that gives a different curve on the graph, an example would be:

$$-\lambda \int (t^2 + t) dt \quad (6)$$

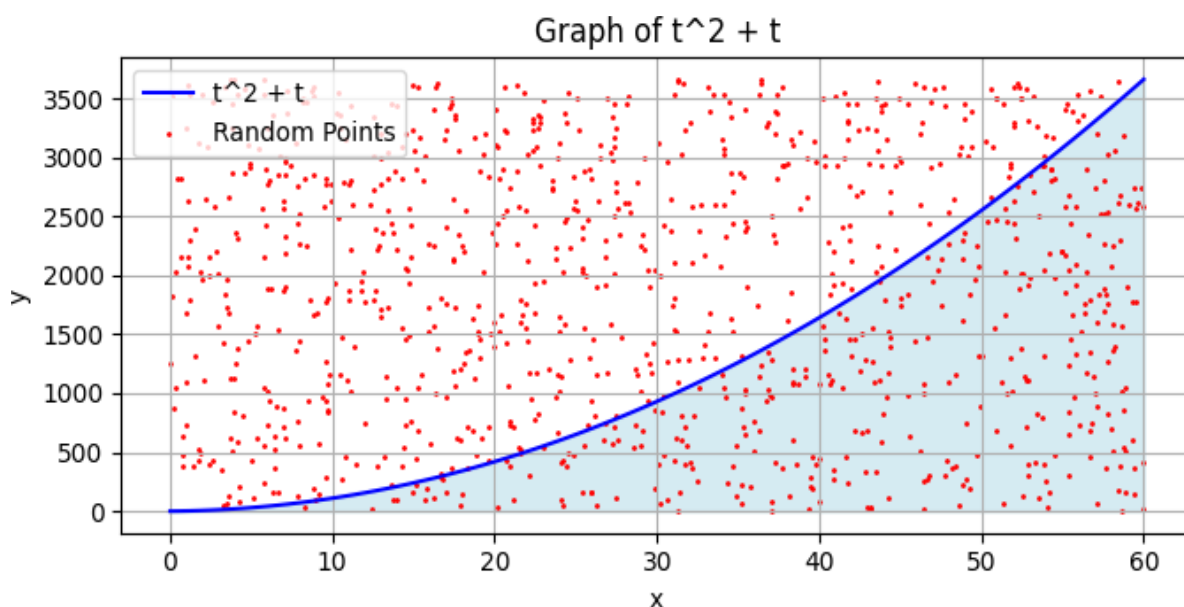


Fig 6.2. Graph of polynomial curve using Monte Carlo integration

### 7.2.3. Scenario Of Sin Function Integration

Assuming that the decay constant changes based on the involvement of the main element and its daughter nuclei. This could create a specific curve. Considering the sin curve for example. The following would be the equation:

$$-\int (\int \sin x \cdot dx) t \cdot dt \quad (8)$$

**Algorithm 2** Algorithm to calculate simple integration of  $(t_2 + t) \cdot dt$

Using Monte-Carlo Approximation

0: Read the number of iterations from command-line argument

1: Define the range of integration

2: Initialize variables

3: Create a random number generator 4: Perform Monte Carlo approximation 5: for 0 to iter do

6: Generate a random value in the range  $[0, 60]$

7: Scale the random value to the range of integration

8: Evaluate the function  $t + t_2$  and add it to the sum

9: Calculate the approximate integral

10: Print the result

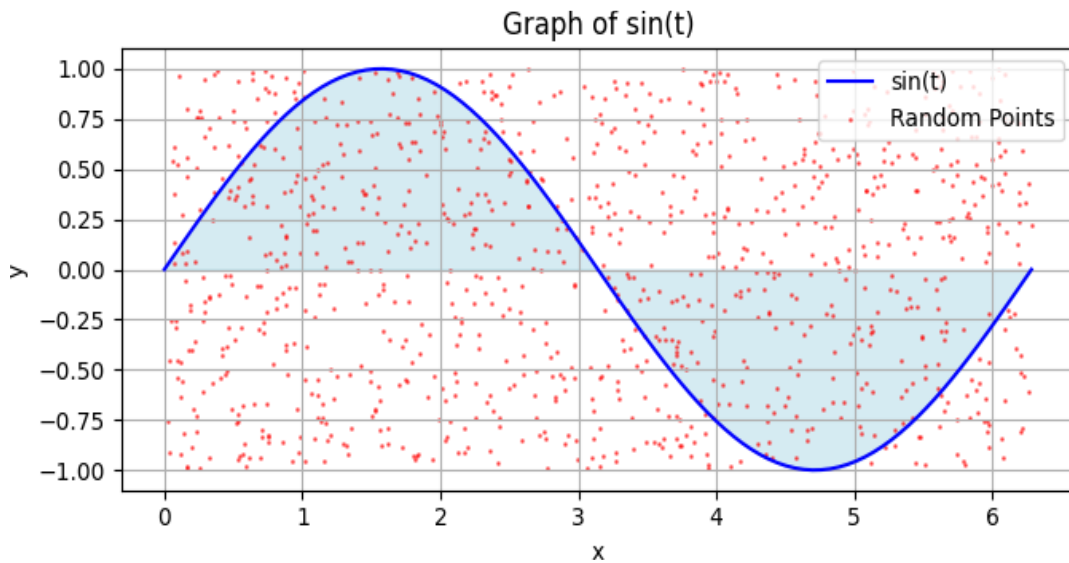


Fig 6.3. Graph of sin curve with Monte Carlo integration

**Algorithm 3** Algorithm to calculate simple integration of  $\sin(t).dt$  using Monte Carlo Approximation 0:

Read the number of iterations from command-line argument

0: Read the number of iterations from command-line argument

1: Define the range of integration

2: Initialize variables

3: Create a random number generator

4: Perform Monte Carlo approximation

5: for 0 to iter do

6: Generate a random value in the range  $[0, 1]$

7: Scale the random value to the range of integration

8: Evaluate the function  $\sin(t)$  and add it to the sum

9: Calculate the approximate integral

10: Print the result



# Chapter 8

## IMPLEMENTATION AND RESULT

We utilized a range of software tools and technologies to accomplish our objectives. Firstly, we employed the Windows 11 operating system, which provided a stable and efficient environment for our development and research activities. The user-friendly interface and robust features of Windows 11 greatly facilitated our work and ensured smooth operation throughout the project.

For Java development, we relied on two powerful integrated development environments (IDEs), namely IntelliJ and Eclipse. These IDEs offered a comprehensive set of tools, including code editing, debugging, and project management features, which greatly enhanced our productivity. We are grateful to the developers of IntelliJ and Eclipse for creating such exceptional platforms for Java development.

To implement the fully homomorphic encryption (FHE) functionalities in our project, we leveraged the FHE Libraries developed by Ziroh Labs. These libraries provided a valuable resource, offering efficient and reliable implementations of FHE algorithms. The support and assistance provided by Ziroh Labs were instrumental in our successful integration of FHE into our research work. We important their specific libraries which aided in the application of integration. For integration specifically, we used the Monte Carlo method as explained in the previous chapter.

Java Swing, a powerful framework for building graphical user interfaces (GUIs) in Java, played a crucial role in developing an intuitive and user-friendly interface for our application. The extensive collection of UI components and the flexibility of Java Swing enabled us to design and present our integration calculations in a visually appealing and interactive manner.

Furthermore, we employed Python, a versatile programming language, for generating graphs and visualizations to represent our research findings. Python's rich ecosystem of libraries, such as Matplotlib, empowered us to create insightful and informative graphs that effectively

conveyed the results of our integration calculations.

8.1.

Function	Expected Results	Actual Results	Accuracy
$-\lambda \int t \cdot dt$	-207.36	- 207.349223	99.99480275848765
$-\lambda \int (t^2 + t) dt$	-8501.76	- 8506.23970	99.94730855728696
$-\int (\int \sin x \cdot dx) t \cdot dt$	-827.46	-826.02388	99.82644236579411

### INTEGRATION ACCURACY

The expected and actual values for the first simple integration function are extremely similar, with an accuracy of 99.99 percent. This high level of precision shows that the calculation's integrity was effectively maintained using FHE. The little disparity between expected and actual findings may be due to the approximations and inherent constraints of numerical integration techniques. However, FHE shows that it is capable of approximating the integration result with accuracy.

**Table of Accuracy:**

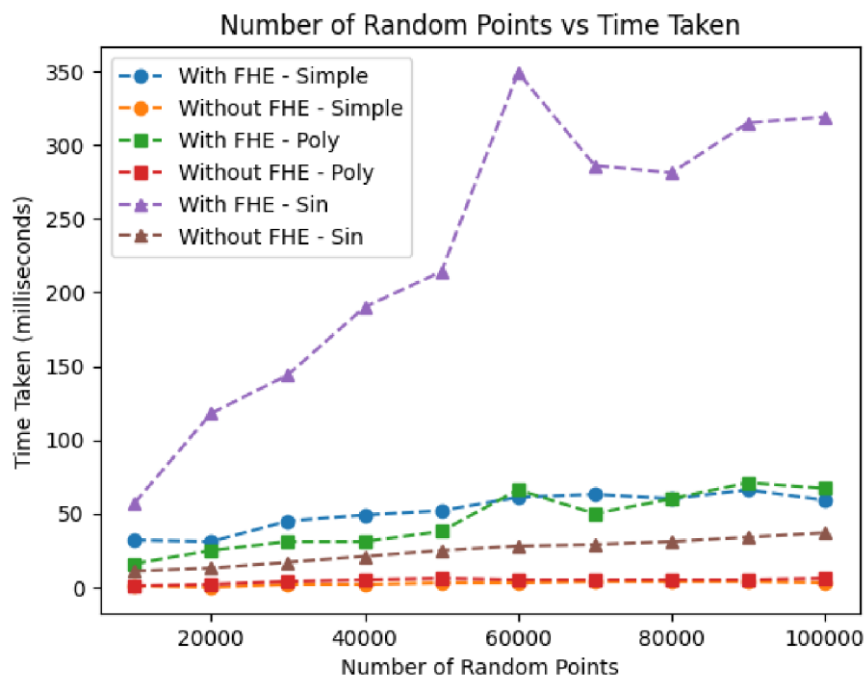


Fig.8.1 Graph representing the time needed for every integration equation to be solved with FHE and without FHE.

With regard to the second polynomial integration function, there is a minor difference between the predicted and observed outcomes and an accuracy of 99.95 percent. This suggests that FHE caused an insignificant mistake in the calculation. Even if the deviation is apparent it's crucial to remember that integration calculations frequently entail complicated mathematical processes, and even small changes in the way the computation is done might affect the outcome. In spite of this, FHE continues to offer a high level of accuracy, demonstrating its efficiency in upholding precision.

With regard to the second function with sin and single variable integration an accuracy of 99.83 percent displays a greater gap between the expected and actual results. Compared to the other cases, the accuracy in this particular case is somewhat lower. The function's fundamental complexity nested integration introduces additional difficulties that could compromise the correctness of the FHE results. The bigger divergence that was seen could be explained by the cumulative effect of the approximations used during the computation.

Overall, the comparative analysis emphasizes the trade- off between the FHE's encryption and privacy-preserving capabilities and the accuracy of the results. FHE still retains a high level of accuracy, ranging from 99.83 percent to 99.99 percent in the examples given, even though it might cause minor deviations in the findings compared to conventional integration computations.

**Tables for time difference between FHE and no FHE:**

**For Simple Function:**

Number of Random Points	Time taken without FHE (in ms)	Time taken with FHE (in ms)
10000	1	32
20000	0	31
30000	2	45
40000	2	49
50000	3	52
60000	3	61
70000	4	63
80000	4	60
90000	4	66
100000	3	59

**For Polynomial Function:**

Number of Random Points	Time taken without FHE (in ms)	Time taken with FHE (in ms)
10000	1	16
20000	2	25
30000	4	31
40000	5	31
50000	6	38
60000	5	66
70000	5	50
80000	5	60
90000	5	71

100000	6	67
--------	---	----

**For Sin Function:**

Number of Random Points	Time taken without FHE (in ms)	Time taken with FHE (in ms)
10000	11	57
20000	13	118
30000	17	144
40000	21	190
50000	25	214
60000	28	349
70000	29	286
80000	31	281
90000	34	315
100000	37	319

**8.2.GUI Implementation using Java Swing**

Java Swing can be used to build a graphical user interface (GUI) for accepting input from random points and displaying the final calculations with and without Fully Homomorphic Encryption (FHE) in the project that implements FHE for integration calculations using Monte Carlo methods. Java Swing can be used for this purpose in the following ways:

- Java Swing offers an extensive collection of components for GUI development. To visualise the findings, the GUI may have features like buttons, labels, text fields, and graphical elements. The layout can be changed to include buttons to start the calculations, input areas for choosing the amount of random points, and FHE encryption settings.
- The GUI may have text fields or sliders where the user may enter the quantity

of random points they want the Monte Carlo algorithm to create. The integration calculation module generates the required number of random points for the Monte Carlo simulation after the user clicks the "Calculate" button on the GUI.

- **Results display:** After the integration computations are completed, the GUI can show the outcomes. It is possible to display the estimated values for both the FHE-based integration and non-FHE integration using Swing components like labels or text fields. Additionally, to aid in better comprehension and analysis, graphical elements like charts or plots can be used to graphically portray the results.
- **Options for FHE Integration:** The GUI can offer switches to enable or disable FHE encryption. The user can select whether to do integration calculations with or without FHE using checkboxes or radio buttons. FHE encryption ensures privacy and confidentiality during the integration process by encrypting the input data and intermediate calculations.
- **The project can offer a user-friendly interface** that enables users to input the number of random points, choose FHE encryption parameters, and visualise the integration calculations by using Java Swing for GUI development. By allowing users to compare the results achieved with and without FHE encryption and facilitating interaction, the GUI improves usability and demonstrates the advantages of privacy-preserving computations in the context of integration calculations utilising Monte Carlo methods.

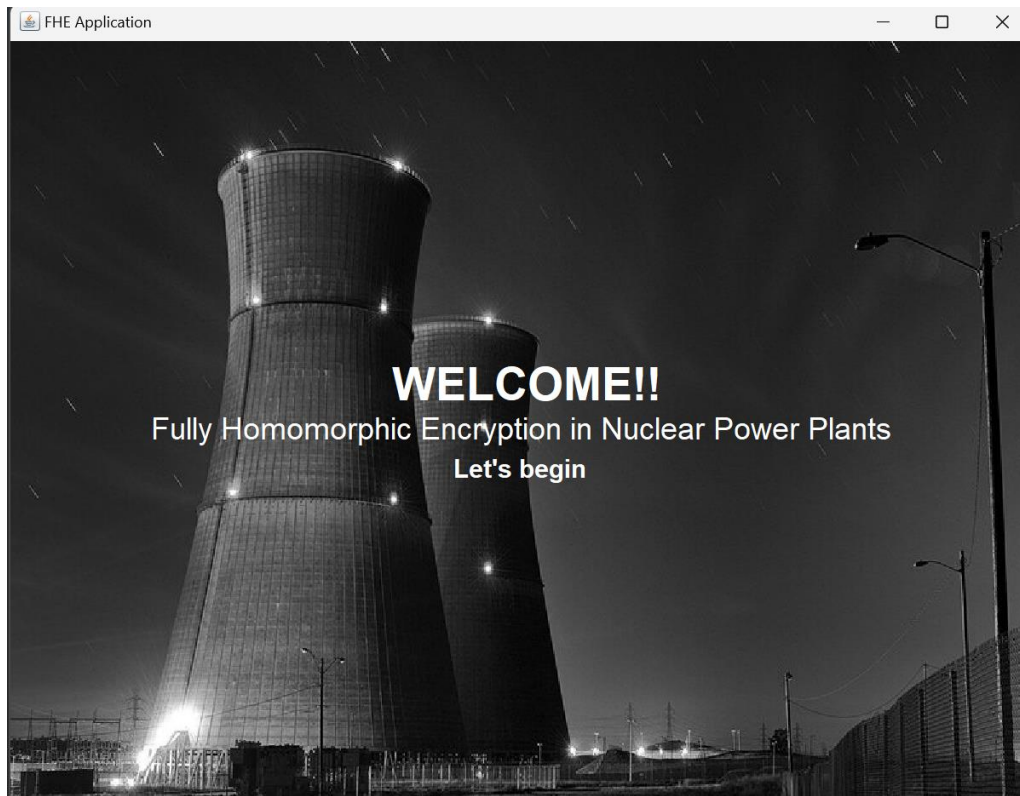


Fig. 8.2. GUI Main screen for user to begin

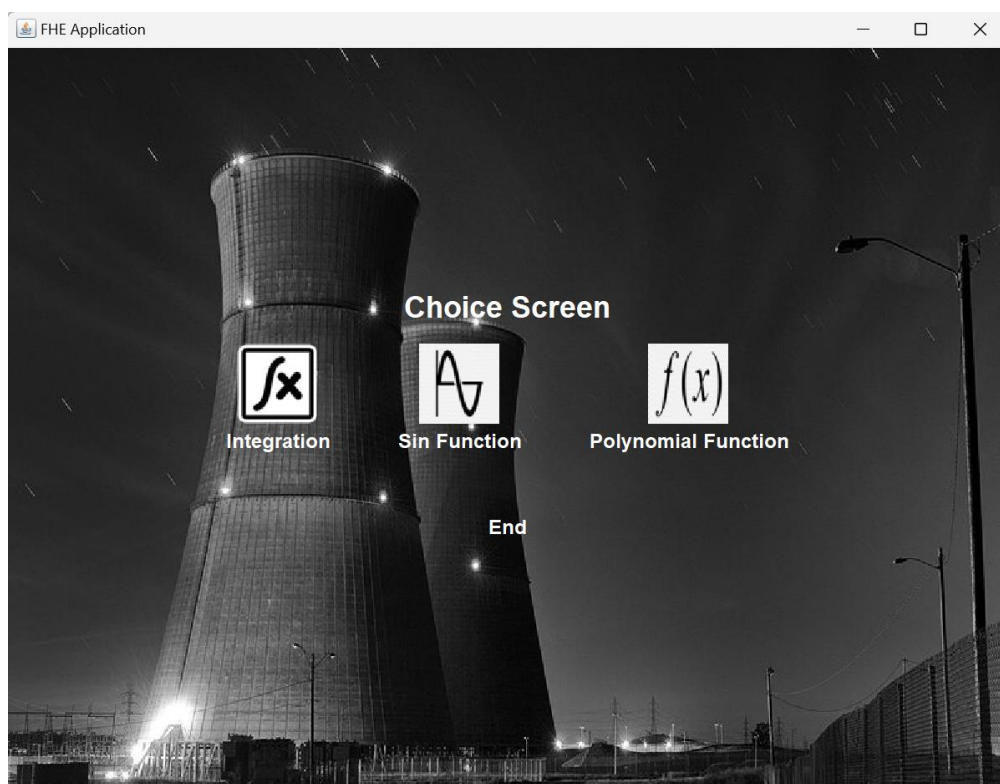


Fig. 8.3. GUI Choice screen for user to select which type of integration they want to perform.

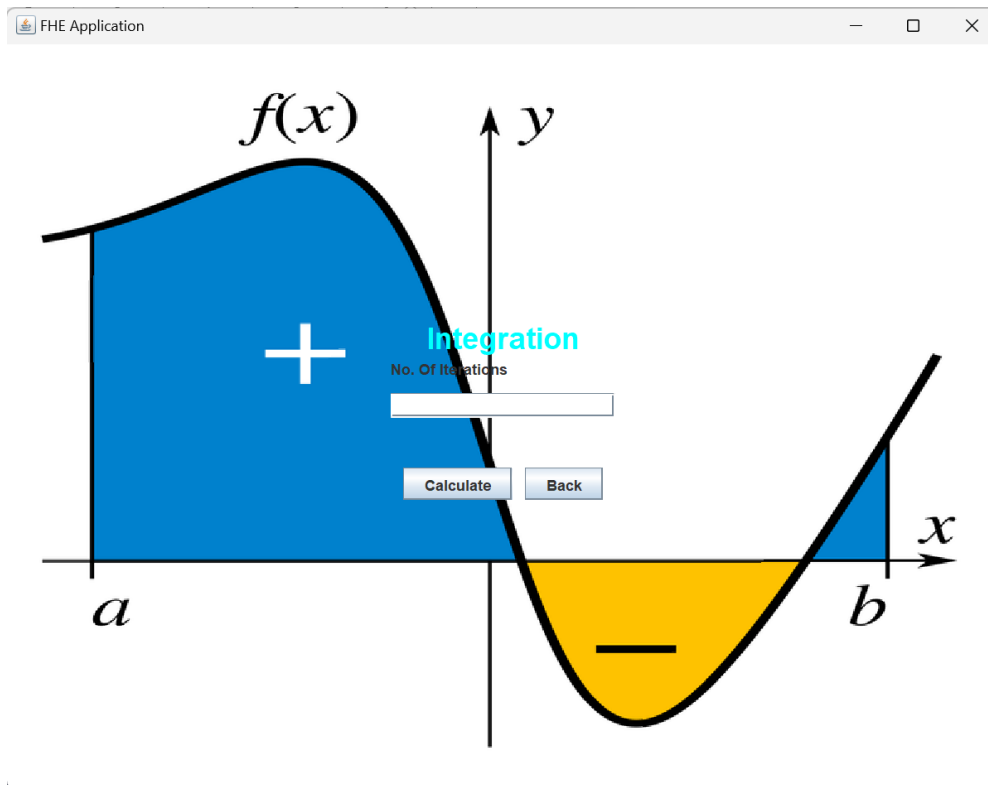


Fig. 8.4. GUI Input screen asking user to enter no. of random points  $t$  generate.

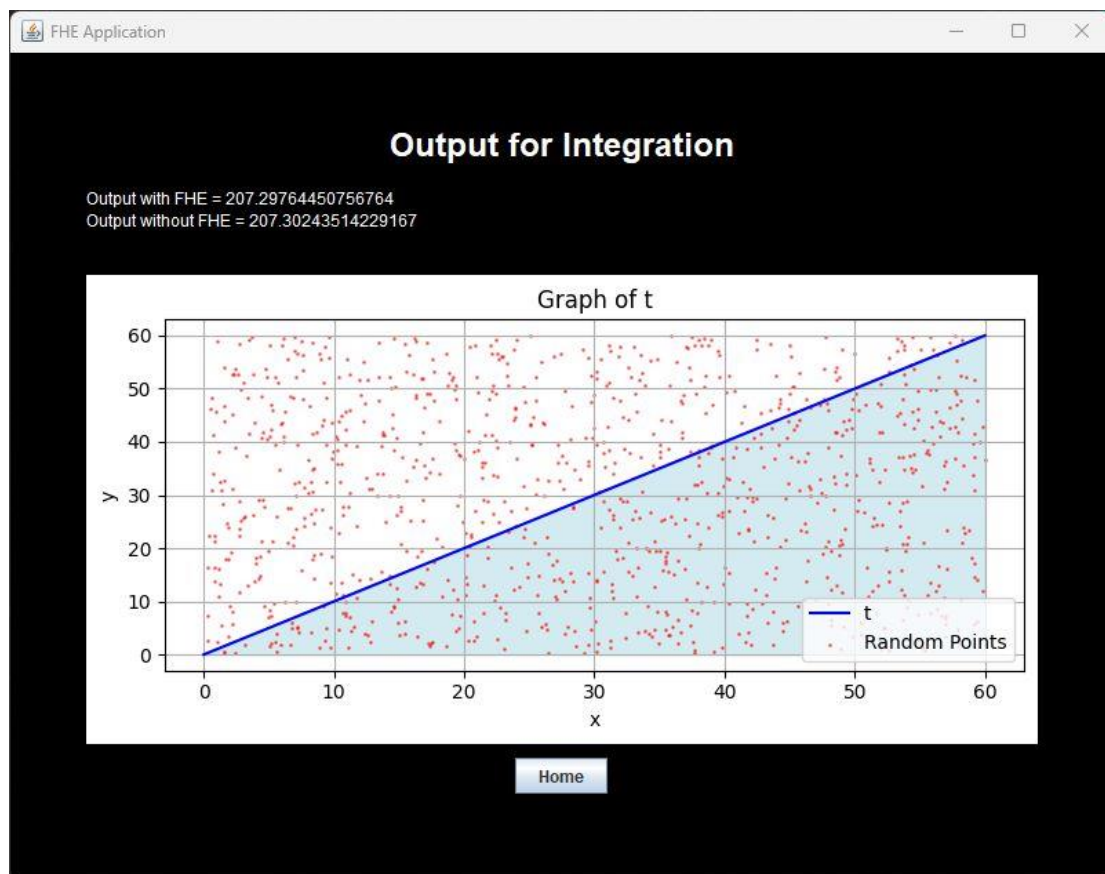


Fig. 8.5. GUI Output screen with integration result using FHE



### 8.3. ADVANTAGES

**Privacy protection:** To ensure that the decay constant is kept secret during the integration process, FHE allows calculation on encrypted data. Sensitive information about certain radioactive elements and their use in power plants can be kept secret through decay constant encryption, reducing the possibility of unauthorized access or potential security breaches.

**Data security:** With FHE, sensitive data such as the decay constant and other relevant details can always remain encrypted, even during computation. By protecting the encrypted data from unauthorized disclosure, modification, or theft, data security is enhanced by reducing the possibility of data breaches or attacks on nuclear power plant systems.

**Computational Efficiency:** FHE systems have improved significantly in terms of computing power, enabling real-time processing and widespread use. The use of FHE enables the rapid execution of integration procedures on encrypted data, including the decay constant, thereby minimizing any negative impact on the overall operational performance of the power plant. Besides this, Nuclear Power Plant generate enough revenue to be able to afford the cost of using FHE in the long run.

**Secure collaboration:** Researchers, engineers and regulators involved in nuclear power plants can safely work together thanks to FHE. Different parties can collaborate while maintaining data secrecy by performing calculations on encrypted data, thus jointly analyzing and interpreting the integrated results without gaining direct access to the private decay constant.

**Regulatory compliance:** The regulations and compliance standards for nuclear power plants are very strict. By providing a secure and privacy-compliant method of processing sensitive data, FHE can help meet these requirements while ensuring that power plant operations remain compliant with legal and regulatory requirements.

## Chapter 9

### **FUTURE PROSPECTS**

Homomorphic Encryption (HE) holds significant promise for the future of secure and privacy-preserving data processing in nuclear power plants. As technology advances and research progresses, several key future aspects can be envisioned for the application of homomorphic encryption in this context:

#### **Enhanced Performance:**

One area of focus for the future of homomorphic encryption in nuclear power plants is improving its performance. Currently, homomorphic encryption schemes, such as Fully Homomorphic Encryption (FHE), involve computational overhead and increased processing times. Ongoing research aims to develop more efficient algorithms, optimization techniques, and hardware accelerators to reduce the computational complexity and enhance the performance of homomorphic encryption schemes. These advancements would enable faster computations on encrypted data and facilitate real-time analysis and decision-making in nuclear power plants.

#### **Scaling Capabilities:**

Another future aspect involves scaling the application of homomorphic encryption to handle large-scale data processing requirements in nuclear power plants. As data volumes continue to grow, the ability to efficiently process and analyze massive datasets while maintaining privacy becomes crucial. Future developments in homomorphic encryption should focus on scalability, allowing for parallelization, distributed computing, or cloud-based solutions to handle the computational demands of large-scale data processing in nuclear power plants.

#### **Integration with Data Analytics and Machine Learning:**

The future of homomorphic encryption in nuclear power plants lies in its integration with advanced data analytics and machine learning techniques. By enabling secure computations on encrypted data, homomorphic encryption can facilitate the application of data analytics

algorithms and machine learning models without compromising data privacy. This opens up possibilities for more sophisticated analysis, anomaly detection, predictive maintenance, and optimization of plant operations. Future research will explore the integration of homomorphic encryption with data-driven techniques to unlock valuable insights while ensuring the confidentiality of sensitive data.

### **Trustworthy Outsourcing of Computations:**

Homomorphic encryption offers the potential for secure and privacy-preserving outsourcing of computations to third-party service providers or cloud environments. Future advancements in homomorphic encryption will focus on enhancing the security and trustworthiness of these outsourcing scenarios. This includes developing protocols and techniques for secure data transfer, verifying the integrity of the computations performed by the service provider, and maintaining the confidentiality of the data throughout the outsourcing process. This aspect can enable nuclear power plants to leverage external computing resources while retaining control over their sensitive data.

### **Regulatory Standards and Compliance:**

As homomorphic encryption gains traction in nuclear power plants, there will be a need for regulatory standards and guidelines specific to its implementation. Future developments will involve the establishment of best practices, industry standards, and regulatory frameworks to ensure the secure and compliant use of homomorphic encryption in the nuclear power industry. These standards will address encryption protocols, key management, auditing, and compliance requirements to provide a robust foundation for the application of homomorphic encryption in nuclear power plants.

### **Collaboration and Knowledge Sharing:**

The future of homomorphic encryption in nuclear power plants also relies on collaboration and knowledge sharing between industry stakeholders, research institutions, and cryptography experts. Continuous collaboration will foster advancements in encryption techniques, algorithmic optimizations, and practical implementation strategies. Sharing knowledge, experiences, and lessons learned will facilitate the adoption and successful integration of homomorphic encryption in nuclear power plant environments.

Overall, the future of homomorphic encryption in nuclear power plants is driven by the pursuit

of improved performance, scalability, integration with data analytics and machine learning, trustworthy outsourcing, regulatory compliance, and collaborative efforts. These future aspects will shape the application of homomorphic encryption, enabling secure and privacy-preserving data processing while maintaining the highest standards of operational safety and integrity in nuclear power plants.

# Chapter 10

## LIMITATIONS

Some key limitations are[18]:

1. Computational Overhead:

FHE operations are computationally intensive and require significant computational resources. Performing complex calculations on encrypted data using FHE can result in a substantial increase in processing time compared to traditional computations on plaintext data. In a time-sensitive environment like a nuclear power plant, this overhead may pose challenges for real-time monitoring and control systems.

2. Latency:

The additional computational overhead of FHE can introduce latency, causing delays in processing and decision-making. In critical scenarios where quick responses are required, such as safety-related events in a nuclear power plant, the increased latency introduced by FHE may not be desirable

3. Complexity and Development Costs:

Implementing FHE in a nuclear power plant system requires expertise in both cryptography and the specific requirements of the plant. FHE is a complex technology, and developing and integrating it into existing systems can be challenging and expensive. Adequate training and expertise would[18] be needed for the staff responsible for implementing and maintaining the FHE system.

4. Compatibility:

FHE relies on specific algorithms and protocols that may not be directly compatible with existing systems and software used in nuclear power plants. Adapting the plant's infrastructure to support FHE may require significant modifications to the existing systems, which could be costly and time-consuming.

### 5. Reliability and Security Concerns:

FHE is a relatively new technology, and while it offers strong security guarantees, its practical implementations may still have vulnerabilities. Ensuring the reliability and robustness of FHE systems in a high-stakes environment like a nuclear power plant is crucial. Thorough testing, verification, and validation processes would be necessary to mitigate any potential risks[18].

Given these limitations, it's important to carefully evaluate the trade-offs and assess the specific requirements and constraints of a nuclear power plant before considering the integration of FHE. It may be more practical to focus on other security measures and encryption techniques that provide an appropriate balance between security, performance, and compatibility with existing systems.

# Chapter 11

## CONCLUSION

In summary, full homomorphic encryption (FHE) offers a breakthrough means to solve the data security and privacy issues in nuclear power plants. When performing integration operations, operational data secrecy can be maintained by using FHE to hide the decay constant and sensitive data. Privacy, data security, computational efficiency, secure collaboration and regulatory compliance are some of the benefits of FHE in this situation. The potential for FHE in nuclear power plants is promising for the future. Key areas of advancement include improvements in cryptographic methods, integration with machine learning, secure remote monitoring, privacy-preserving data sharing, and industry-wide adoption through standardization. These developments can improve operational safety, optimize plant performance, promote secure communications and ensure regulatory compliance.

The application of homomorphic encryption in nuclear reactors holds significant promise for enhancing data security, privacy, and computational capabilities within these critical facilities. As technology continues to advance, there are several avenues for further exploration and development in this field. The following future scope highlights potential areas of focus: **Advanced Cryptographic Techniques:** As the field of cryptography continues to be studied and developed, FHE systems may evolve, which will lead to more effective and secure encryption techniques. The performance and profitability of FHE can be improved by advances in encryption algorithms and protocols, allowing for greater use and integration into nuclear power plant operations.

**Integration with machine learning and AI:** The combination of FHE with methods of machine learning and AI can open new ways to decrypt and analyse encrypted data in nuclear power plants. To improve asset optimization, predictive maintenance and security, it may be possible to extract valuable insights from encrypted data by applying secure machine learning algorithms while protecting the privacy of sensitive data.

**Secure remote monitoring:** FHE makes it easier and safer to remotely monitor the operation of nuclear power plants. The risk of unauthorized access or data leakage during transmission can be reduced by encrypting, processing and processing the data locally at the power plant and only transmitting the encrypted insights. This allows regulators or other authorized bodies to monitor activities effectively and securely, ensuring compliance and protecting the privacy.

**Data exchange while respecting privacy:** FHE can enable the secure and data protection-protecting data exchange between different research institutions or nuclear power plants. While maintaining the confidentiality of specific power plant data, encrypted data can be securely analysed and integrated to enable collaborative research, benchmarking and knowledge sharing. This can lead to improvements in the safety, efficiency and operation of nuclear power plants without compromising data protection.

**Standardization and Industry Adoption:** There is an opportunity for standardization initiatives within the nuclear power industry as FHE continues to evolve and become widely accepted as a viable solution to privacy and security. Establishing industry standards and guidelines can accelerate the introduction of FHE in nuclear power plant operations, ensure interoperability and create a framework for secure and confidential handling of data.



# Chapter 12

## References

- [1] Craig Gentry. 2009. A fully homomorphic encryption scheme. Ph.D. Dissertation. Stanford University, Stanford, CA, USA. Advisor(s) Dan Boneh. Order Number: AAI3382729.
- [2] Ducas, L., Micciancio, D. (2014). Improved Short Lattice Signatures in the Standard Model. In: Garay, J.A., Gennaro, R. (eds) *Advances in Cryptology – CRYPTO 2014*. CRYPTO 2014. Lecture Notes in Computer Science, vol 8616. Springer, Berlin, Heidelberg. <https://doi.org/10.1007/978-3-662-44371-2-19>
- [3] R. Sendhil and A. Amuthan, "A Descriptive Study on Homomorphic Encryption Schemes for Enhancing Security in Fog Computing," 2020 International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2020, pp. 738-743, doi: 10.1109/ICOSEC49089.2020.9215422.
- [4] Z. H. Mahmood and M. K. Ibrahim, "A Noise-Free Homomorphic Encryption based on Chaotic System," 2020 1st. Information Technology To Enhance e-learning and Other Application (IT-ELA, Baghdad, Iraq, 2020, pp. 132-137, doi: 10.1109/IT-ELA50150.2020.9253124.
- [5] A. Bel Korchi and N. El Mrabet, "A Practical Use Case of Homomorphic Encryption," 2019 International Conference on Cyberworlds (CW), Kyoto, Japan, 2019, pp. 328-335, doi: 10.1109/CW.2019.00060.
- [6] J. West, J. Hale, M. Papa and P. Hawrylak, "Automatic Identification of Critical Digital Assets," 2019 2nd International Conference on Data Intelligence and Security (ICDIS), South Padre Island, TX, USA, 2019, pp. 219-224, doi: 10.1109/ICDIS.2019.00040.
- [7] I. Syafalni et al., "Cloud Security Implementation using Homomorphic Encryption," 2020 IEEE International Conference on Communication, Networks and Satellite (Comnetsat), Batam, Indonesia, 2020, pp. 341- 345, doi: 10.1109/Comnetsat50391.2020.9328979.
- [8] D. Jung, J. Shin, C. Lee, K. Kwon and J. T. Seo, "Cyber Security Controls in Nuclear Power Plant by Technical Assessment Methodology," in *IEEE Access*, vol. 11, pp. 15229-15241, 2023, doi: 10.1109/ACCESS.2023.3244991.
- [9] Y. Guo, A. Yan and J. Wang, "Cyber Security Risk Analysis of Physical Protection Systems of Nuclear Power Plants and Research on the Cyber Security Test Platform Using Digital Twin Technology," 2021 International Conference on Power System Technology (POWERCON), Haikou, China, 2021, pp. 1889-1892, doi: 10.1109/POWERCON53785.2021.9697764.
- [10] S. Kim, S. Kim, K. -h. Nam, S. Kim and K. -h. Kwon, "Cyber Security Strategy for Nuclear Power Plant through Vital Digital Assets," 2019 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 2019, pp. 224-226, doi: 10.1109/CSCI49370.2019.00045.
- [11] J. -h. Roh, S. -k. Lee, C. -W. Son, C. Hwang, J. Kang and J. Park, "Cyber Security System with FPGA-based Network Intrusion Detector for Nuclear Power Plant," *IECON 2020 The 46th Annual Conference of the IEEE Industrial Electronics Society*, Singapore, 2020, pp. 2121- 2125, doi: 10.1109/IECON43393.2020.9255158.
- [12] R. Awadallah and A. Samsudin, "Homomorphic Encryption for Cloud Computing and Its Challenges,"

2020 IEEE 7th International Conference on Engineering Technologies and Applied Sciences (IC-ETAS), Kuala Lumpur, Malaysia, 2020, pp. 1-6, doi: 10.1109/IC-ETAS51660.2020.9484283.

[13] N. N. Kucherov, M. A. Deryabin and M. G. Babenko, "Homomorphic Encryption Methods Review," 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIconRus), St. Petersburg and Moscow, Russia, 2020, pp. 370-373, doi: 10.1109/EIconRus49466.2020.9039110.

[14] Z. H. Mahmood and M. K. Ibrahim, "New Fully Homomorphic Encryption Scheme Based on Multistage Partial Homomorphic Encryption Applied in Cloud Computing," 2018 1st Annual International Conference on Information and Sciences (AiCIS), Fallujah, Iraq, 2018, pp. 182-186, doi: 10.1109/AiCIS.2018.00043.

[15] N. Jain, K. Nandakumar, N. Ratha, S. Pankanti and U. Kumar, "Optimizing Homomorphic Encryption based Secure Image Analytics," 2021 IEEE 23rd International Workshop on Multimedia Signal Processing (MMSP), Tampere, Finland, 2021, pp. 1-6, doi: 10.1109/MMSP53017.2021.9733620.

[16] S. Mittal, K. R. Ramkumar and A. Kaur, "Preserving Privacy in Clouds using Fully Homomorphic Encryption," 2021 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON), Pune, India, 2021, pp. 1-7, doi: 10.1109/SMART-GENCON51891.2021.9645822.

[17] A. Poletykin, V. Promyslov, E. Jharko and K. Semenov, "Risk Assessment and Cyber Security of Nuclear Power Plants," 2022 15th International Conference Management of large-scale system development (MLSD), Moscow, Russian Federation, 2022, pp. 1-5, doi: 10.1109/MLSD55143.2022.9934271.

[18] A. Viand, P. Jattke and A. Hithnawi, "SoK: Fully Homomorphic Encryption Compilers," 2021 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2021, pp. 1092-1108, doi: 10.1109/SP40001.2021.00068.

[19] M. V. Ramana, "Small Modular and Advanced Nuclear Reactors: A Reality Check," in IEEE Access, vol. 9, pp. 42090-42099, 2021, doi: 10.1109/ACCESS.2021.3064948.

[20] A. Poletykin, V. Promyslov, E. Jharko and K. Semenov, "Risk Assessment and Cyber Security of Nuclear Power Plants," 2022 15th International Conference Management of large-scale system development (MLSD), Moscow, Russian Federation, 2022, pp. 1-5, doi: 10.1109/MLSD55143.2022.9934271.

[21] J. -h. Roh, S. -k. Lee, C. -W. Son, C. Hwang, J. Kang and J. Park, "Cyber Security System with FPGA-based Network Intrusion Detector for Nuclear Power Plant," IECON 2020 The 46th Annual Conference of the IEEE Industrial Electronics Society, Singapore, 2020, pp. 2121-2125, doi: 10.1109/IECON43393.2020.9255158.

[22] R. L. A. Tavares, R. d. O. Albuquerque and W. F. Giozza, "Effectiveness evaluation of a nuclear facility security system under a cyber-physical attack scenario," 2022 17th Iberian Conference on Information Systems and Technologies (CISTI), Madrid, Spain, 2022, pp. 1-6, doi: 10.23919/CISTI54924.2022.9820179.

[23] Y. Guo, A. Yan and J. Wang, "Cyber Security Risk Analysis of Physical Protection Systems of Nuclear Power Plants and Research on the Cyber Security Test Platform Using Digital Twin Technology," 2021 International Conference on Power System Technology (POWERCON), Haikou, China, 2021, pp. 1889-1892, doi: 10.1109/POWERCON53785.2021.9697764

[24] Z. H. Mahmood and M. K. Ibrahim, "New Fully Homomorphic Encryption Scheme Based on Multistage Partial Homomorphic Encryption Applied in Cloud Computing," 2018 1st Annual International Conference on Information and Sciences (AiCIS), Fallujah, Iraq, 2018, pp. 182-186, doi: 10.1109/AiCIS.2018.00043.

[25] S. Kim, S. Kim, K. -h. Nam, S. Kim and K. -h. Kwon, "Cyber Security Strategy for Nuclear Power Plant

## Fully Homomorphic Encryption in Nuclear Power Plants

through Vital Digital Assets," 2019 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 2019, pp. 224-226, doi: 10.1109/CSCI49370.2019.00045.

# Chapter 13

## APPENDICES

### 13.1. Base Paper

---

2019 International Conference on Cyberworlds (CW)

---

## A practical use case of homomorphic encryption

Amina BEL KORCHI<sup>(1,2)</sup> and Nadia EL MRABET<sup>(1)</sup>

(1) Mines Saint-Etienne, CEA-Tech, Centre CMP, Departement SAS, F - 13541 Gardanne  
France Amina.BelKorchi@kontron.com and nadia.el-mrabet@emse.fr

(2) Kontron, La Garde, France

Abstract This paper is a proof of concept that homomorphic encryption can be deployed in practice and can be used by the industry to ensure security and computation of customer data. In this paper, we present a concrete use case of homomorphic encryption that is not considered in literature, using Fan and Vercauteren (FV) cryptosystem, and we propose a practical implementation of FV cryptosystem and its deployment in an IoT use case. Keywords: IoT use case, cloud security, anonymity, homomorphic encryption

978-1-7281-2297-7/19/\$31.00 ©2019 IEEE  
DOI 10.1109/CW.2019.00060

with practical depths to use homomorphic encryption in practice.

Those practical security schemes are based on LWE [10] (Learning with errors) and RLWE [11] (Ring Learning with Errors) problems.

In this paper, we give a practical use case of homomorphic encryption, we validate our scheme using a home made implementation of FV cryptosystem and provide the detailed description of this use case and the description of our implementation.

In the first section of the paper, we define the use case. Then, in the second section, we give the description of FV cryptosystem. In the third section, we describe existing implementations of FV, and finally we introduce our implementation with its performances inside the cloud, the gateway and inside an administrator machine.

#### I. INTRODUCTION

Nowadays, data security has become a very important subject for the industries to improve business. They need to manipulate data, while ensuring data protection, privacy and anonymization.

Homomorphic Encryption (HE) responds to this challenge and enables calculations on encrypted data without decryption. Let  $E(a)$  and  $E(b)$  be the encryption of  $a$  and  $b$  using an homomorphic cryptosystem,  $E(a)$  and  $E(b)$  verify the following properties:  $E(a) \oplus E(b) = E(a \oplus b)$  and  $E(a) \times E(b) = E(a \times b)$ .

Two variants of homomorphic encryption exist: Fully Homomorphic Encryption (FHE) and Somewhat Homomorphic Encryption (SWHE). FHE is a fully homomorphic encryption allowing the evaluation of an arbitrary circuit, as to SWHE, it can evaluate circuits of constant depth. The circuit depth is the number of multiplication that can be performed using a given scheme. Exceeding this depth, decryption can not be done correctly due to the noise that appears during the encryption of plaintexts. This noise grows after every ciphertext multiplication until we reach a level where we can not decrypt correctly.

Gentry [1] has invented the first FHE cryptosystem in 2009 using a bootstrapping [1] procedure to transform a SWHE cryptosystem into a FHE cryptosystem. The security of Gentry's scheme is based on ideal lattices [2]. The bootstrapping technique transforms a ciphertext resulting from a circuit to a new ciphertext with a noise similar to the one in a ciphertext freshly encrypted.

Numerous schemes have been proposed following Gentry's cryptosystem [3], [4], [5], basing their security on different hardness assumptions.

Before the apparition of the technique to turn bootstrapping in less than 0.1 seconds [6], the inconvenient of FHE schemes was the time to turn the bootstrapping, this is the reason why different SWHE schemes as [7], [8], [9] have been developed


#### II. IOT USE CASE

Homomorphic encryption is a solution to solve the main problems of IoT [12]: security, storage and computations. Assume a use case in IoT where we have different devices, several gateways and a cloud with multiple servers to store and manage data. Each gateway receives several messages from sensors, encrypts messages homomorphically and sends them to the cloud. For our case the cloud will store those ciphertexts and makes some calculations based on addition and multiplication of collected data at different time and in various geographies.

The protocol used for sending messages from sensors to the gateway is LORA [13] (Long Range Wireless Protocol). The cloud includes a MQTT [14] server (Publish/Subscribe protocol). To store data in the cloud, the gateway sends a publish command, and to receive a data from the cloud, the calculation server sends a subscribe command. This scenario is shown in Figure 1.

We can also describe a scenario where different supermarkets of different companies need to store and compute the number of product sales in the context of stock management. The goal of these companies is to store in the cloud the encryption of this data without revealing their identities due to the competition. In the cloud we can compute the sum of sales of each product in order to supply the stock of supermarkets if necessary. Let us picture a use case in seaport to accelerate the shipments of products through customs by expecting enough trucks

## 13.2. Plagiarism Reports

**Similarity Report ID:** oid:28480:35805971

---

PAPER NAME  
**Capstone Report.pdf**

---

WORD COUNT <b>12635 Words</b>	CHARACTER COUNT <b>76421 Characters</b>
PAGE COUNT <b>51 Pages</b>	FILE SIZE <b>1.1MB</b>
SUBMISSION DATE <b>May 20, 2023 5:25 PM GMT+5:30</b>	REPORT DATE <b>May 20, 2023 5:26 PM GMT+5:30</b>

---

● **14% Overall Similarity**  
The combined total of all matches, including overlapping sources, for each database.

- 5% Internet database
- 6% Publications database
- Crossref database
- Crossref Posted Content database
- 11% Submitted Works database

● **Excluded from Similarity Report**

- Bibliographic material



Report: Capstone\_Project\_Report

# Capstone\_Project\_Report

by Whos in paris

## General metrics

86,043	11,935	818	47 min 44 sec	1 hr 31 min
characters	words	sentences	reading time	speaking time

## Score



This text scores better than 95% of all texts checked by Grammarly

## Writing Issues

324	93	231
Issues left	Critical	Advanced

## Plagiarism

✓ This text seems 100% original. Grammarly found no matching text on the Internet or in ProQuest's databases.

### Project to Outcome mapping

Objectives:

1. To maintain confidentiality of data at every point in the implementation.
2. To focus on secure passing of data within calculations
3. To achieve accuracy in results through calculation performed on encrypted data using Fully Homomorphic Encryption
4. To facilitate a user-friendly performance of the source-code along with GUI

Sr. No.	PRN No.	Student Name	Individual Project Student Specific Objective	Learning Outcomes mapped
1	1032191063	Hritika Kalghatgi	To perform Integration Operations using FHE.	
2	1032191332	Anshul Jaiswal	To perform Integration Operations using FHE.	
3	1032192138	Kushagra Amlani	To Design a Graphical User Interface.	
4	1032191624	Khush Advani	To Design a Graphical User Interface.	



Dr. Vishwanath Karad  
**MIT WORLD PEACE**  
**UNIVERSITY** | PUNE  
TECHNOLOGY, RESEARCH, SOCIAL INNOVATION & PARTNERSHIPS

**Individual Project Report**

on

**Fully Homomorphic Encryption In Nuclear Power Plants**

**Module : Implementation of Fully Homomorphic Encryption in Integration  
using Monte Carlo algorithm.**

Submitted by

**Hritika Kalghatgi**

**1032191063**

Under the Internal Guidance of

**Dr. Sukhada Bhingarkar**

Under the External Guidance of

**Dr. Hrishikesh Dewan**

**School of Computer Engineering and Technology**

**MIT World Peace University, Kothrud,**

**Pune 411 038, Maharashtra - India**

**2022-2023**



# PROBLEM STATEMENT

Implementing Fully Homomorphic Encryption for Integration Calculations in Nuclear Power Plants using Monte Carlo Methods.

Nuclear power facilities must use sensitive data that must be shielded from unauthorized access and disclosure in order to execute integration calculations. Traditional encryption techniques make it difficult to execute computations directly on encrypted data, necessitating the decryption of confidential material, which is risky from a security standpoint. To ensure privacy and data protection while maintaining the accuracy of the integration results, a framework for integration must be created that uses Fully Homomorphic Encryption (FHE) to perform calculations on encrypted data.

I have focused on using Monte Carlo Method with my team to produce genuine and positive results.

# MODULE OBJECTIVES

Create an integration framework that uses FHE techniques to carry out computations on encrypted data, protecting the privacy and confidentiality of sensitive data used in nuclear power plant integration calculations.

Implement Monte Carlo Integration Methods to enable precise and effective calculations. In order to do this, random sample generation, function evaluation, and result comparison is involved.

To safeguard the integrity and confidentiality of the sensitive data used in integration computations, implement strong encryption and decryption modules utilizing FHE methods. To ensure the secure development, storage, and distribution of encryption keys, use secure key management procedures such as separation of the code into Client and Server.

Validate and Assess Performance: To ensure the precision and effectiveness of the FHE-based integration calculations, carry out extensive testing and performance assessments. To evaluate the effect of FHE on computational performance, compare the outcomes with those of conventional, non-encrypted integration calculations.

This project I want to be able to offer a safe and privacy-preserving solution for integration calculations in nuclear power plants by meeting the aforementioned problem description and objectives. An improvement in safety and operational effectiveness in nuclear power plants will result from the successful application of FHE techniques and Monte Carlo methods, which will guarantee the secrecy of sensitive data while retaining the accuracy and efficiency of integration calculations.

# MODULE SCOPE

The following major components make up the module scope for the project outlined in the problem statement:

Fully Homomorphic Encryption (FHE) functions in classes: Focuses on applying FHE methods to calculations on encrypted data. It involves the use of FHE algorithms for encryption and decryption, safe key generation and management, and project integration of the FHE libraries or frameworks.

Implementing Monte Carlo techniques for integration calculations: It involves generating random points by taking user input, finding the area under the curve, and assessing various functions. The FHE functions are used to execute the integration computations on the encrypted data.

The performance and accuracy of the integration computations: I have tested and evaluated this using outputs for different random points generated. Creating test cases, doing integration testing, and contrasting the outcomes of FHE-based integration calculations with conventional, non-encrypted integration calculations are all included in this process. Evaluations of performance rate the computational effectiveness of the FHE-based strategy has also been observed by creating graphs.

The project activities, including the system architecture, implementation details, importing of external libraries, and operational processes, which I have compiled in a research paper. It also includes producing technical specifications and explanations of algorithms. This module also includes reporting on the project's development, results, and discoveries by me.

# MODULE

## 4.1 Hardware & Software Requirements:

### Hardware Requirements:

- High-performance servers or systems capable of running the homomorphic encryption algorithms with minimal latency and maximum throughput.
- Sufficient storage capacity to store encrypted and decrypted data.
- Robust network infrastructure to ensure secure and reliable data transmission.

### Software Requirements:

- Operating system: Linux (Ubuntu or CentOS) or Windows Server 2016 or higher.
- Homomorphic encryption libraries: Ziroh Labs Secure Numeric homomorphic encryption library
- Programming language: Python, C++, or Java.
- Development tools: IDEs such as PyCharm or Eclipse, version control systems such as Git or SVN, and code review tools such as Gerrit or Crucible.
- Tools/Libraries for making required graphs: Tableau and Python Matplotlib

## 4.2. Module Interfaces:

- Interface to enter user input in the form of double, for taking the number of random points as input from the user.
- Client interface for generation of Key and for performing encryption and decryption of data using that key.
- Server interface for performing the required arithmetic operations and calculations on the encrypted data using FHE.
- Output interface to display the output to the user.
- Python interface with matplotlib for generating required graphs.

## 4.3. Module Dependencies

- Java Version 8 and above

- Ziroh Labs' SecureNumeric Library for implementing FHE.
- SecureNumeric-1.0.jar
- SecureNumericClient-1.0.jar
- Java.util.\* packages for in-built functions.
- Separate Client.java class for key generation and encryption/decryption.
- Separate Server.java class for performing arithmetic operations.
- Python version 2.6 and above.
- Jupyter / Google Colab Notebook
- Python numpy library
- Python matplotlib library.

## 4.4. Module Design:

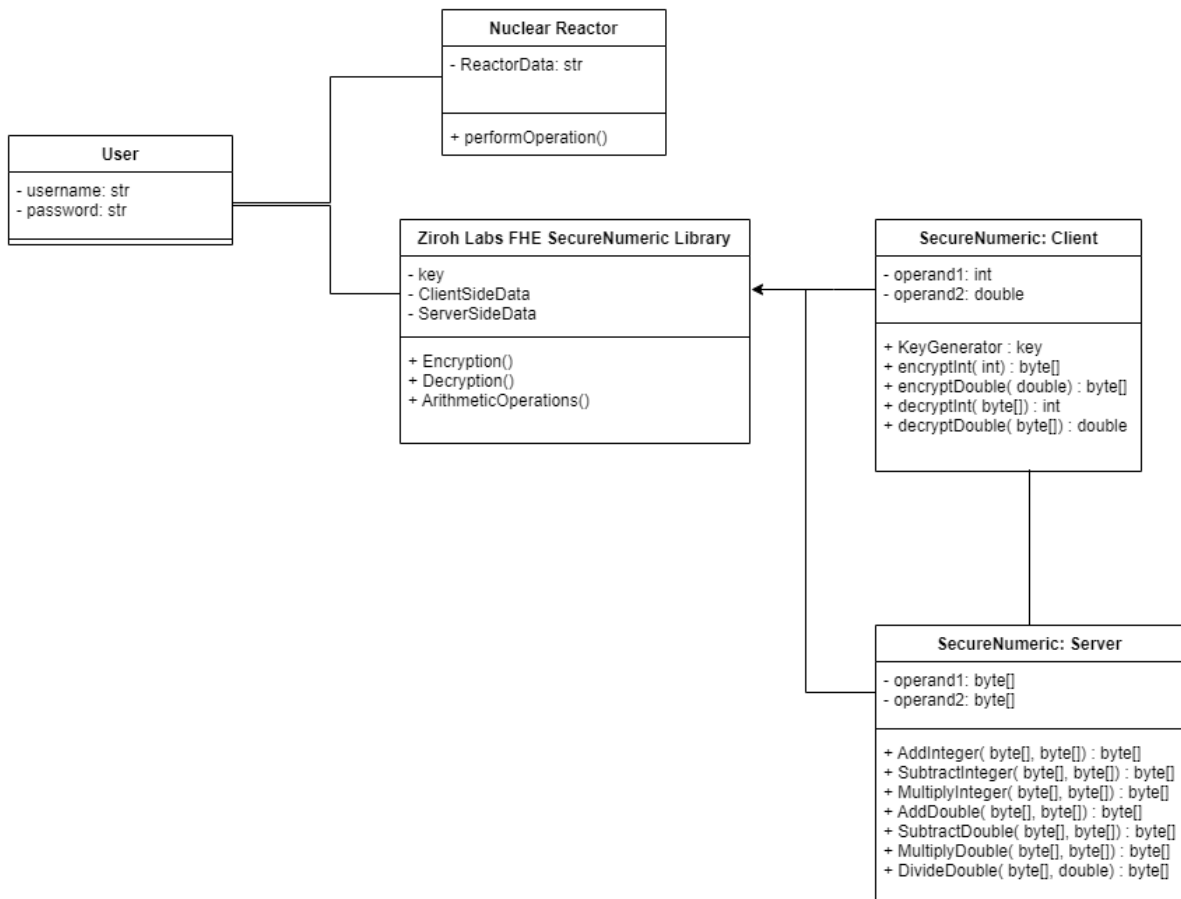


Fig 4.1. Class Diagram of Module

## 4.5. Implementation

I have used FHE to encrypt the decay constant and have integration performed on calculating the decay factor. Every step involved is encrypted with no decryption happening at anything stage. There are three scenarios with variations in simple integration equations which I have stated below.

The very first scenario to consider would be one in which I have a specific decay constant of a single element. The amount of the element would vary depending upon the decay factor which is given by the following formula:

$$e^{-\lambda t} \quad (1)$$

Here,  $\lambda$  is the decay constant and 't' is the time over which I want to find the amount of element decayed.

The remaining nuclei fraction equal to the decay factor:

$$\frac{N(t)}{N(0)} = e^{-\lambda t} \quad (2)$$

$N(t)$  is the amount of nuclei after decaying and  $N(0)$  is the amount of nuclei at the beginning.

This can be further written as:

$$\int \frac{N(t)}{N(0)} dN(t) = \int e^{-\lambda t} \cdot dt \quad (3)$$

$$\ln \left( \frac{N(t)}{N(0)} \right) = -\int \lambda t \cdot dt \quad (4)$$

Considering the above equation, I am able to calculate the log of fraction of remaining nuclei by using:

$$-\int \lambda t \cdot dt \quad (5)$$

### 4.5.1. Scenario Of Simple Integration:

If the decay constant does not change as I am only considering a single element in the scenario, I could integrate the following over time:

$$-\lambda \int t \cdot dt \quad (6)$$

Here is the algorithm for calculating the simple integral of  $t \cdot dt$  using Monte Carlo approximation:

**Algorithm 1** Algorithm to calculate simple integration of  $t \cdot dt$  using Monte Carlo Approximation

0: Read the number of iterations from command-line argument

1: Define the range of integration

2: Initialize variables

3: Create a random number generator 4: Perform Monte Carlo approximation 5: for 0 to tier do

6: Generate a random value in the range  $[0, 60]$

7: Scale the random value to the range of integration

8: Evaluate the function  $t$  and add it to the sum

9: Calculate the approximate integral

10: Print the result

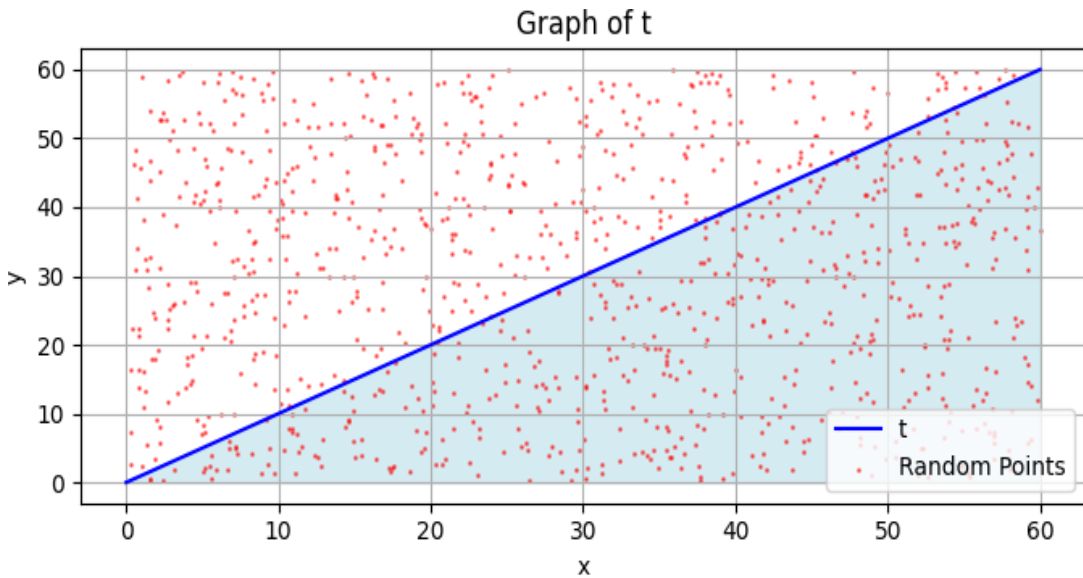


Fig 4.2. Graph of simple single variable curve using Monte Carlo integration

#### 4.5.2. Scenario Of Polynomial Integration

To consider a more complex equation that gives a different curve on the graph, an example would be:

$$-\lambda \int (t^2 + t) dt \quad (6)$$

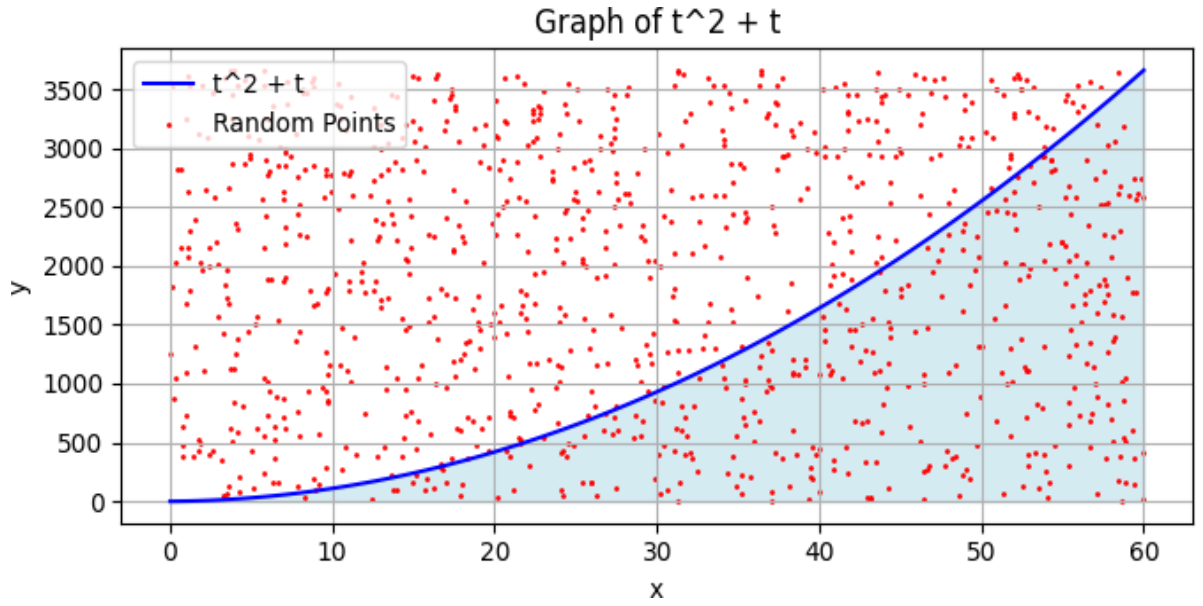


Fig 4.3. Graph of polynomial curve using Monte Carlo integration

#### 4.5.3. Scenario Of Sin Function Integration

Assuming that the decay constant changes based on the involvement of the main element and its daughter nuclei. This could create a specific curve. Considering the sin curve for example. The following would be the equation:

$$-\int (\int \sin x \cdot dx) t \cdot dt \quad (8)$$

**Algorithm 2** Algorithm to calculate simple integration of  $(t^2 + t) \cdot dt$

Using Monte-Carlo Approximation

- 0: Read the number of iterations from command-line argument
- 1: Define the range of integration
- 2: Initialize variables
- 3: Create a random number generator
- 4: Perform Monte Carlo approximation
- 5: for 0 to iter do
- 6: Generate a random value in the range [0, 60]
- 7: Scale the random value to the range of integration
- 8: Evaluate the function  $t + t^2$  and add it to the sum



9: Calculate the approximate integral

10: Print the result

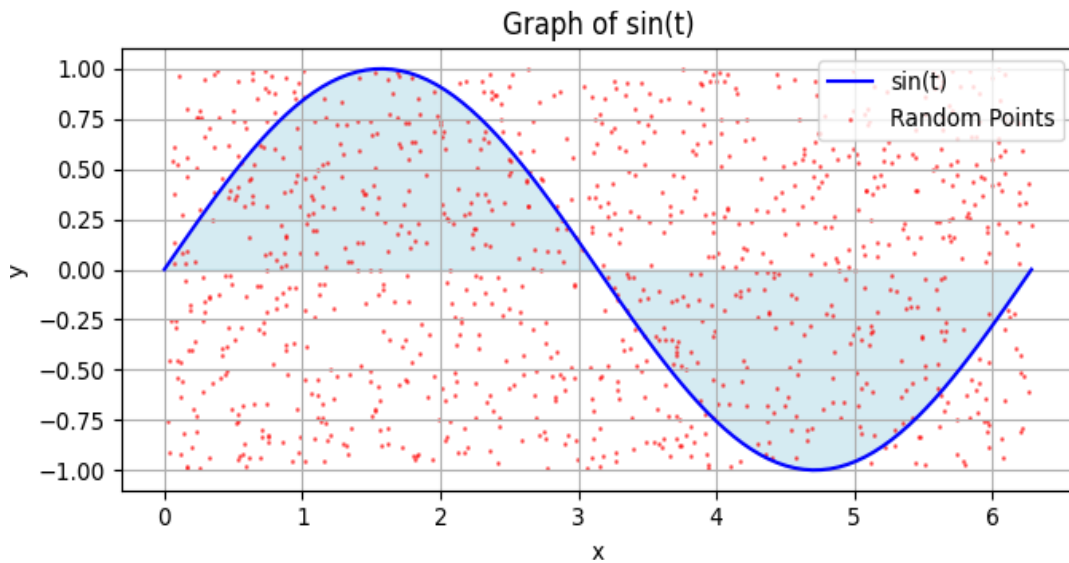


Fig 4.4. Graph of sin curve with Monte Carlo integration

**Algorithm 3** Algorithm to calculate simple integration of  $\sin(t).dt$  using Monte Carlo Approximation 0:

Read the number of iterations from command-line argument

0: Read the number of iterations from command-line argument

1: Define the range of integration

2: Initialize variables

3: Create a random number generator

4: Perform Monte Carlo approximation

5: for 0 to iter do

6: Generate a random value in the range  $[0, 1]$

7: Scale the random value to the range of integration

8: Evaluate the function  $\sin(t)$  and add it to the sum

9: Calculate the approximate integral

10: Print the result

## 4.6. TESTING & RESULT

I utilized a range of software tools and technologies to accomplish our objectives. Firstly, I employed the Windows 11 operating system, which provided a stable and efficient environment for our development and research activities. The user-friendly interface and robust features of Windows 11 greatly facilitated our work and ensured smooth operation throughout the project.

For Java development, I relied on two powerful integrated development environments (IDEs), namely IntelliJ and Eclipse. These IDEs offered a comprehensive set of tools, including code editing, debugging, and project management features, which greatly enhanced our productivity. I am grateful to the developers of IntelliJ and Eclipse for creating such exceptional platforms for Java development.

To implement the fully homomorphic encryption (FHE) functionalities in our project, I leveraged the FHE Libraries developed by Ziroh Labs. These libraries provided a valuable resource, offering efficient and reliable implementations of FHE algorithms. The support and assistance provided by Ziroh Labs were instrumental in our successful integration of FHE into our research work. I imported their specific libraries which aided in the application of integration. For integration specifically, I used the Monte Carlo method as explained in the previous chapter.

Java Swing, a powerful framework for building graphical user interfaces (GUIs) in Java, played a crucial role in developing an intuitive and user-friendly interface for our application. The extensive collection of UI components and the flexibility of Java Swing enabled us to design and present our integration calculations in a visually appealing and interactive manner.

Furthermore, I employed Python, a versatile programming language, for generating graphs and visualizations to represent our research findings. Python's rich ecosystem of libraries, such as Matplotlib, empowered us to create insightful and informative graphs that effectively conveyed the results of our integration calculations.

#### 4.6.1. INTEGRATION ACCURACY

The expected and actual values for the first simple integration function are extremely similar, with an accuracy of 99.99 percent. This high level of precision shows that the calculation's integrity was effectively maintained using FHE. The little disparity between expected and actual findings may be due to the approximations and inherent constraints of numerical integration techniques. However, FHE shows that it is capable of approximating the integration result with accuracy.

**4.1 Table of Accuracy:**

Function	Expected Results	Actual Results	Accuracy
$-\lambda \int t \cdot dt$	-207.36	- 207.349223	99.99480275848765
$-\lambda \int (t^2 + t) dt$	-8501.76	- 8506.23970	99.94730855728696
$-\int (\int \sin x \cdot dx) t \cdot dt$	-827.46	-826.02388	99.82644236579411

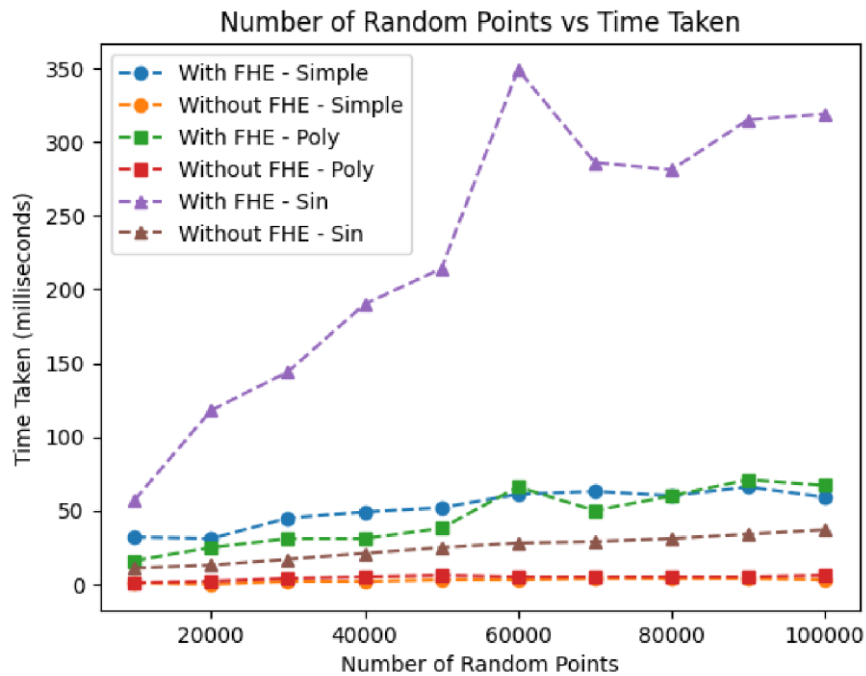


Fig.4.5 Graph representing the time needed for every integration equation to be solved with FHE and without FHE.

With regard to the second polynomial integration function, there is a minor difference between the predicted and observed outcomes and an accuracy of 99.95 percent. This suggests that FHE caused an insignificant mistake in the calculation. Even if the deviation is apparent it's crucial to remember that integration calculations frequently entail complicated mathematical processes, and even small changes in the way the computation is done might affect the outcome. In spite of this, FHE continues to offer a high level of accuracy, demonstrating its efficiency in upholding precision.

With regard to the second function with sin and single variable integration an accuracy of 99.83 percent displays a greater gap between the expected and actual results. Compared to the other cases, the accuracy in this particular case is somewhat lower. The function's fundamental complexity nested integration introduces additional difficulties that could compromise the correctness of the FHE results. The bigger divergence that was seen could be explained by the cumulative effect of the approximations used during the computation.

Overall, the comparative analysis emphasizes the trade- off between the FHE's encryption and privacy-preserving capabilities and the accuracy of the results. FHE still retains a high level of accuracy, ranging from 99.83 percent to 99.99 percent in the examples given, even though it might cause minor deviations in the findings compared to conventional integration computations.

**4.2 Tables for time difference between FHE and no FHE:****For Simple Function:**

Number of Random Points	Time taken without FHE (in ms)	Time taken with FHE (in ms)
10000	1	32
20000	0	31
30000	2	45
40000	2	49
50000	3	52
60000	3	61
70000	4	63
80000	4	60
90000	4	66
100000	3	59

**For Polynomial Function:**

Number of Random Points	Time taken without FHE (in ms)	Time taken with FHE (in ms)
10000	1	16
20000	2	25
30000	4	31
40000	5	31
50000	6	38
60000	5	66
70000	5	50
80000	5	60
90000	5	71
100000	6	67

**For Sin Function:**

Number of Random Points	Time taken without FHE (in ms)	Time taken with FHE (in ms)
10000	11	57
20000	13	118
30000	17	144
40000	21	190
50000	25	214
60000	28	349
70000	29	286
80000	31	281
90000	34	315
100000	37	319

## CONCLUSION

In summary, the proposed project seeks to address the difficulties associated with combining fully homomorphic encryption (FHE) approaches and Monte Carlo techniques for secure integration computations in nuclear power plants. By utilising FHE, the project maintains the accuracy and effectiveness of the outcomes while protecting the privacy and security of sensitive data used in integration computations. The project's scope is made up of the FHE module, the Monte Carlo integration module, the security module, the testing and evaluation module, and the documentation and reporting module. These modules provide a thorough foundation for secure and privacy-preserving integration calculations. By enhancing data security, privacy, and operational effectiveness in nuclear power plants, this project's successful implementation will ultimately increase safety and preserve regulatory compliance in the sector.